PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-111679
(43)Date of publication of application : 30.04.1996

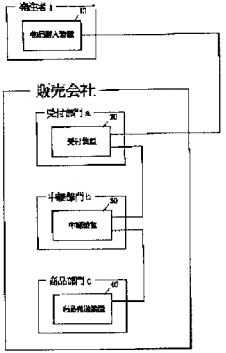
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G06F 17/60
G09C 1/00

(21)Application number : 06-245571
(22)Date of filing : 11.10.1994

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : OMORI MOTOJI
TATEBAYASHI MAKOTO

(54) MAIL ORDER SYSTEM

(57)Abstract:
PURPOSE: To surely protect the privacy of an ordering person concerning the mail order system for ordering and purchasing merchandise through a communication network.
CONSTITUTION: An ordering person (i) doubly ciphers the merchandise code of order merchandise by using two cryptographic keys and those two cryptographic keys are respectively ciphered for a relay section (b) and a merchandise section (c). Then, the doubly ciphered merchandise code is transmitted to a reception section (a) together with the two ciphered cryptographic keys and the identifier of the ordering person. The reception section (a) transmits the received ciphered order contents to the relay section (b) together with a reference number Ref 1. Among the received ciphered order contents, the cryptographic key ciphered for the relay section is deciphered and the doubly ciphered merchandise code is partially deciphered by the delay section (b). Then, the partially deciphered merchandise code is transmitted to the merchandise section (c) together with the cryptographic key ciphered for the merchandise section and a reference number Ref 2. The merchandise section (c) deciphers the cryptographic key ciphered for the merchandise section, further deciphers the partially deciphered merchandise code and recognizes the name of ordered merchandise.



LEGAL STATUS

[Date of request for examination] 10.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]	
[Patent number]	3496774
[Date of registration]	28.11.2003
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－111679

(43)公開日　平成８年(1996)４月30日

(51)Int.Cl.[6]	識別記号	ＦＩ
Ｈ04Ｌ 9/00		
9/10		
9/12		
		Ｈ04Ｌ 9/00　Ｚ
		Ｇ06Ｆ 15/21　330

審査請求　未請求　請求項の数９　ＯＬ　（全33頁）　最終頁に続く

(21)出願番号　特願平6－245871

(22)出願日　平成６年(1994)10月11日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

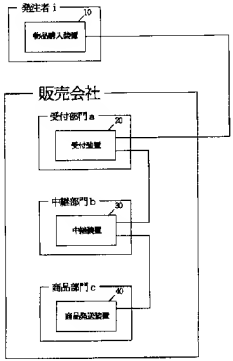
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】通信販売システム

(57)【要約】　（修正有）

【目的】　通信ネットワークを介して商品を注文購入する通信販売システムにおいて、発注者のプライバシーを確実に保護する。

【構成】　発注者ｉは、発注商品の商品コードを、２つの暗号鍵を用いて二重に暗号化し、その２つの暗号鍵をそれぞれ、中継部門ｂ、商品部門ｃ向けに暗号化する。そして、二重に暗号化した商品コードを、暗号化した２つの暗号鍵および発注者の識別子と共に受付部門ａに送る。受付部門ａは、受信した暗号化発注内容を、照会番号Ｒｅｆ１と共に中継部門ｂに送る。中継部門ｂは、受信した暗号化発注内容のうち、中継部門向けに暗号化された暗号鍵を復号し、二重に暗号化されている商品コードを一部復号する。そして、一部復号された商品コードを、商品部門向けに暗号化された暗号鍵および照会番号Ｒｅｆ２と共に商品部門ｃへ送る。商品部門ｃは、商品部門向けに暗号化された暗号鍵を復号して、一部復号された商品コードをさらに復号し、発注された商品名を知る。



1

【特許請求の範囲】

【請求項１】　複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、

前記発注者、前記受付部門および前記商品部門には、それぞれ、物品購入装置、受付装置および商品発送装置が設けられており、

前記物品購入装置は、

電子データから成る鍵を発生する鍵発生手段と、

前記鍵を用いて、商品の発注内容を暗号化する発注内容暗号化手段と、

前記鍵を暗号化する鍵暗号化手段と、

前記暗号化された商品の発注内容に、前記暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第１の送信手段とを含み、

前記受付装置は、

前記物品購入装置から送信されてくるデータを受信する第１の受信手段と、

前記第１の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、

前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第１の受信手段が受信した前記暗号化された商品の発注内容と前記暗号化された鍵とに、前記発注者の識別情報とは異なる仮名情報を付加して、前記商品発送装置に送信する第２の送信手段と、

前記発注者の識別情報と前記仮名情報との対応関係を記憶する対応関係記憶手段とを含み、

前記商品発送装置は、

前記受付装置から送信されてくるデータを受信する第２の受信手段と、

前記第２の受信手段が受信した前記暗号化された鍵を復号する鍵復号手段と、

前記復号された鍵を用いて、前記第２の受信手段が受信した前記暗号化された商品の発注内容を復号する発注内容復号手段と、

前記電子的商品を保管する商品保管手段と、

前記復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、

前記読み出し手段により読み出された電子的商品を、前記復号された鍵を用いて暗号化する商品暗号化手段と、

前記暗号化された電子的商品を、前記第２の受信手段が受信した前記仮名情報と共に、前記受付装置に送信する第３の送信手段とを含み、

前記受付装置は、さらに前記商品発送装置から送信されてくるデータを受信する第３の受信手段と、

前記第３の受信手段が受信した前記仮名情報に基づいて、前記対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、

前記第３の受信手段が受信した前記暗号化された電子的

2

商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第４の送信手段とを含み、

前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項２】　前記仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項１に記載の通信販売システム。

【請求項３】　複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、

前記発注者、前記受付部門、前記中継部門および前記商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、

前記物品購入装置は、

電子データから成る第１および第２の鍵を発生する鍵発生手段と、

前記第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化手段と、

前記第１および第２の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、

前記２重に暗号化された商品の発注内容に、前記暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第１の送信手段とを含み、

前記受付装置は、

前記物品購入装置から送信されてくるデータを受信する第１の受信手段と、

前記第１の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、

前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第１の受信手段が受信した前記２重に暗号化された商品の発注内容と前記暗号化された第１および第２の鍵とに、前記発注者の識別情報とは異なる第１の仮名情報を付加して、前記中継装置に送信する第２の送信手段と、

前記発注者の識別情報と前記第１の仮名情報との対応関係を記憶する第１の対応関係記憶手段とを含み、

前記中継装置は、

前記受付装置から送信されてくるデータを受信する第２の受信手段と、

前記第２の受信手段が受信した前記暗号化された第１の鍵を復号する第１の鍵復号手段と、

前記復号された第１の鍵を用いて、前記第２の受信手段が受信した前記２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号手段と、

前記部分的に復号された商品の発注内容に、前記第１の仮名情報とは異なる第２の仮名情報を付加して、前記商品発送装置に送信する第３の送信手段と、

前記第１の仮名情報と前記第２の仮名情報との対応関係

を記憶する第２の対応関係記憶手段とを含み、
前記商品発送装置は、
前記中継装置から送信されてくるデータを受信する第３の受信手段と、
前記第３の受信手段が受信した前記暗号化された第２の鍵を復号する第２の鍵復号手段と、
前記復号された第２の鍵を用いて、前記第３の受信手段が受信した前記部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号手段と、
前記電子的商品を保管する商品保管手段と、
前記全面的に復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、
前記読み出し手段により読み出された電子的商品を、前記復号された第２の鍵を用いて暗号化する第１の商品暗号化手段と、
前記第２の鍵を用いて暗号化された電子的商品を、前記第３の受信手段が受信した前記第２の仮名情報と共に、前記中継装置に送信する第４の送信手段とを含み、
前記中継装置は、さらに前記商品発送装置から送信されてくるデータを受信する第４の受信手段と、
前記第４の受信手段が受信した前記暗号化された電子的商品を、対応する前記第１の鍵を用いて２重に暗号化する第２の商品暗号化手段と、
前記第４の受信手段が受信した前記第２の仮名情報に基づいて、前記第２の対応関係記憶手段を検索し、当該第２の仮名情報に対応する前記第１の仮名情報を特定する仮名情報特定手段と、
前記第２の鍵を用いて２重に暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第１の仮名情報と共に、前記受付装置に送信する第５の送信手段とを含み、
前記受付装置は、さらに前記中継装置から送信されてくるデータを受信する第５の受信手段と、
前記第５の受信手段が受信した前記第１の仮名情報に基づいて、前記第１の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、
前記第５の受信手段が受信した前記２重に暗号化された電子的商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第６の送信手段とを含み、
前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項４】　前記第１および第２の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項３に記載の通信販売システム。

【請求項５】　複数の発注者、受付部門、ｎ個（ｎは２以上の整数）の中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、
前記発注者、前記受付部門、前記中継部門および前記商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、
前記物品購入装置は、
電子データから成る第１および第２の鍵を発生する鍵発生手段と、
前記第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化手段と、
前記第１および第２の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、
前記２重に暗号化された商品の発注内容に、前記暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第１の送信手段とを含み、
前記受付装置は、
前記物品購入装置から送信されてくるデータを受信する第１の受信手段と、
前記第１の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、
前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第１の受信手段が受信した前記２重に暗号化された商品の発注内容と、前記暗号化された第１および第２の鍵とに、前記発注者の識別情報とは異なる第１の仮名情報を付加して、第１番目の前記中継部門に属する中継装置に送信する第２の送信手段と、
前記発注者の識別情報と前記第１の仮名情報との対応関係を記憶する第１の対応関係記憶手段とを含み、
第１番目の前記中継部門に属する中継装置は、
前記受付装置から送信されてくるデータを受信する第２の受信手段と、
前記第２の受信手段が受信した前記暗号化された第１の鍵を復号する第１の鍵復号手段と、
前記復号された第１の鍵を用いて、前記第２の受信手段が受信した前記２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号手段と、
前記部分的に復号された商品の発注内容に、前記第１の仮名情報とは異なる第２の仮名情報を付加して、第２番目の前記中継装置に属する中継装置に送信する第３の送信手段と、
前記第１の仮名情報と前記第２の仮名情報との対応関係を記憶する第２の対応関係記憶手段とを含み、
第ｍ番目（ｍは、２≦ｍ≦ｎ－１の整数）の前記中継部門に属する中継装置は、
第（ｍ－１）番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第３の受信手段と、
前記第３の受信手段が受信した前記部分的に復号された商品の発注内容に、第ｍの仮名情報とは異なる第（ｍ－１）の仮名情報を付加して、第（ｍ＋１）番目の中継部門に属する中継装置に送信する第４の送信手段と、

5

前記第ｍの仮名情報と前記第（ｍ－１）の仮名情報との対応関係を記憶する第３の対応関係記憶手段とを含み、

第ｎ番目の前記中継部門に属する中継装置は、

第（ｎ－１）番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第４の受信手段と、

前記第４の受信手段が受信した前記部分的に復号された商品の発注内容に、第ｎの仮名情報とは異なる第（ｎ＋１）の仮名情報を付加して、前記商品発送装置に送信する第５の送信手段と、

前記第ｎの仮名情報と前記第（ｎ＋１）の仮名情報との対応関係を記憶する第４の対応関係記憶手段とを含み、

前記商品発送装置は、

第ｎ番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第５の受信手段と、

前記第５の受信手段が受信した前記暗号化された第２の鍵を復号する第２の鍵復号手段と、

前記復号された第２の鍵を用いて、前記第５の受信手段が受信した前記部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号手段と、前記電子的商品を保管する商品保管手段と、

前記全面的に復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、

前記読み出し手段により読み出された電子的商品を、前記復号された第２の鍵を用いて暗号化する第１の商品暗号化手段と、

前記第２の鍵を用いて暗号化された電子的商品を、前記第５の受信手段が受信した前記第（ｎ＋１）の仮名情報と共に、第ｎ番目の前記中継部門に属する中継装置に送信する第６の送信手段とを含み、

第ｎ番目の前記中継部門に属する中継装置は、さらに前記商品発送装置から送信されてくるデータを受信する第６の受信手段と、

前記第６の受信手段が受信した前記第（ｎ＋１）の仮名情報に基づいて、前記第４の対応関係記憶手段を検索し、当該第（ｎ－１）の仮名情報に対応する第ｎの仮名情報を特定する第１の仮名情報特定手段と、

前記第６の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第ｎの仮名情報と共に、第ｎ番目の前記中継部門に属する中継装置に送信する第７の送信手段とを含み、

第ｍ番目の前記中継部門に属する中継装置は、さらに第（ｍ－１）番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第７の受信手段と、

前記第７の受信手段が受信した前記第ｍの仮名情報に基づいて、前記第３の対応関係記憶手段を検索し、当該第ｍの仮名情報に対応する第（ｍ－１）の仮名情報を特定する第２の仮名情報特定手段と、

前記第７の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第

6

（ｍ－１）の仮名情報と共に、第（ｍ－１）番目の前記中継部門に属する中継装置に送信する第８の送信手段とを含み、

第１番目の前記中継部門に属する中継装置は、さらに第２番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第８の受信手段と、

前記第８の受信手段が受信した前記暗号化された電子的商品を、対応する前記第１の暗号鍵を用いて２重に暗号化する第２の商品暗号化手段と、

前記第８の受信手段が受信した前記第２の仮名情報に基づいて、前記第３の対応関係記憶手段を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する第３の仮名情報特定手段と、

前記第８の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第１の仮名情報と共に、前記受付装置に送信する第９の送信手段とを含み、

前記受付装置は、さらに第１番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第９の受信手段と、

前記第９の受信手段が受信した前記第１の仮名情報に基づいて、前記第１の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、

前記第９の受信手段が受信した前記２重に暗号化された電子的商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第６の送信手段とを含み、

前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項６】　複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、

前記発注者においては、

電子データから成る鍵を発生する鍵発生ステップと、

前記鍵を用いて、商品の発注内容を暗号化する発注内容暗号化ステップと、

前記鍵を暗号化する鍵暗号化ステップと、

前記暗号化された商品の発注内容に、前記暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第１の送信ステップとを実行し、

前記受付部門においては、

前記発注者から送信されてくるデータを受信する第１の受信ステップと、

前記第１の受信ステップで受信した前記本人確認情報が、正当なものか否かを確認する確認ステップと、

前記確認ステップによって前記本人確認情報が正当なものと確認された場合、前記第１の受信ステップで受信した前記暗号化された商品の発注内容と前記暗号化された

7

鍵とに、前記発注者の識別情報とは異なる仮名情報を付加して、前記商品発送装置に送信する第２の送信ステップと、

前記発注者の識別情報と前記仮名情報との対応関係を記憶する対応関係記憶ステップとを実行し、

前記商品部門においては、

前記受付部門から送信されてくるデータを受信する第２の受信ステップと、

前記第２の受信ステップで受信した前記暗号化された鍵を復号する鍵復号ステップと、

前記復号された鍵を用いて、前記第２の受信ステップで受信した前記暗号化された商品の発注内容を復号する発注内容復号ステップと、

前記復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が前記受付部門にわからないように梱包封印する梱包封印ステップと、

前記梱包封印された商品を、前記第２の受信ステップで受信した前記仮名情報と共に、前記受付部門に発送する第１の発送ステップとを実行し、

前記受付部門においては、さらに前記商品部門から受け取った前記仮名情報に基づいて、前記対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、

前記商品部門から受け取った前記梱包封印された商品を、前記発注者特定ステップで特定された発注者に発送する第２の発送ステップとを実行することを特徴とする、通信販売方法。

【請求項７】　前記仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項６に記載の通信販売方法。

【請求項８】　複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、

前記発注者においては、

電子データから成る第１および第２の鍵を発生する鍵発生ステップと、

前記第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化ステップと、

前記第１および第２の鍵を、それぞれ別個に暗号化する鍵暗号化ステップと、

前記２重に暗号化された商品の発注内容に、前記暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第１の送信ステップとを含み、

前記受付部門においては、

前記物品購入装置から送信されてくるデータを受信する第１の受信ステップと、

前記第１の受信ステップで受信した前記本人確認情報が、正当なものか否かを確認する確認ステップと、

前記確認ステップによって前記本人確認情報が正当なものと確認された場合、前記第１の受信ステップで受信した前記２重に暗号化された商品の発注内容と前記暗号化された第１および第２の鍵とに、前記発注者の識別情報とは異なる第１の仮名情報を付加して、前記中継装置に送信する第２の送信ステップと、

前記発注者の識別情報と前記第１の仮名情報との対応関係を記憶する第１の対応関係記憶ステップとを実行し、

前記中継部門においては、

前記受付装置から送信されてくるデータを受信する第２の受信ステップと、

前記第２の受信ステップで受信した前記暗号化された第１の鍵を復号する第１の鍵復号ステップと、

前記復号された第１の鍵を用いて、前記第２の受信ステップで受信した前記２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号ステップと、

前記部分的に復号された商品の発注内容に、前記第１の仮名情報とは異なる第２の仮名情報を付加して、前記商品発送装置に送信する第３の送信ステップと、

前記第１の仮名情報と前記第２の仮名情報との対応関係を記憶する第２の対応関係記憶ステップとを実行し、

前記商品部門においては、

前記中継装置から送信されてくるデータを受信する第３の受信ステップと、

前記第３の受信ステップで受信した前記暗号化された第２の鍵を復号する第２の鍵復号ステップと、

前記復号された第２の鍵を用いて、前記第３の受信ステップで受信した前記部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号ステップと、

前記全面的に復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が前記受付部門にわからないように梱包封印する第１の梱包封印ステップと、

前記梱包封印された商品を、前記第２の受信ステップで受信した前記仮名情報と共に、前記中継部門に発送する第１の発送ステップとを実行し、

前記中継部門においては、さらに前記商品部門から受け取った前記梱包封印された商品を、さらに２重に梱包封印する第２の梱包封印ステップと、

前記商品部門から受け取った前記第２の仮名情報に基づいて、前記第２の対応関係記憶ステップで記憶した対応関係を検索し、当該第２の仮名情報に対応する前記第１の仮名情報を特定する仮名情報特定ステップと、

前記２重に梱包封印された商品を、前記仮名情報特定ステップにより特定された前記第１の仮名情報と共に、前記受付部門に発送する第２の発送ステップとを実行し、

前記受付部門においては、さらに前記中継部門から受け取った前記第１の仮名情報に基づいて、前記第１の対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、

前記中継部門から受け取った前記２重に梱包封印された

8

9

商品を、前記発注者特定ステップにより特定された発注者に発送する第３の発送ステップとを実行することを特徴とする、通信販売方法。

【請求項９】　前記第１および第２の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項８に記載の通信販売方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信販売システムに関し、より特定的には、通信ネットワークを用いて、商品の発注と流通を行うシステムに関する。

【０００２】

【従来の技術】近年、市場ではカタログを用いた通信販売による物品の売買が盛んになってきており、徐々に販売高を伸ばしている。また、パーソナルコンピュータ（以下、パソコンと略称する）通信などのネットワーク網が普及してきており、電話における口頭での受け渡しではどうしても聞違いが出るような大量かつ詳細な情報も、パソコン通信では正確に伝えられることもあって、パソコン通信を用いた通信ネットワークを用いた通信販売が、大いに発展しつつある。特に、コンピュータの業務用ソフトウェアやゲーム用ソフトウェア、そしてマルチメディア電子百科辞典などの電子的商品が、頻繁に取り引きされている。さらに、パソコン通信、ディジタルＣＡＴＶ網、Ｂ－ＩＳＤＮ網などの通信ネットワークを用いた通信販売網で、電子的商品の販売や情報サービスの提供が多く行われつつある。この場合、もちろん無形商品である電子的商品は、発注を受けたネットワーク網を介して発注者の元に送られる。

【０００３】図１５は、従来の通信ネットワークを用いた通信販売システムの構成を示す図である。図１５において、初めに、各発注者５は、販売会社６に、名前とパソコン通信アドレスと振替指定銀行口座などを記した通信販売システム申込書を送り、銀行には、販売会社から正当な請求があった場合には、その口座から口座所有者の許可なしに振り替えても構わないという内容の契約書を送っておく。この手続きにより、発注者５は、本システムにおける発注者識別子ＵＩＤを得る。

【０００４】図１５において、発注者５と販売会社６は、パソコン通信でつながっている。発注者５は、電子的商品を販売会社６に発注し、販売会社６から送られてくる電子的商品を受け取る物品購入装置５０を所持している。当該物品購入装置５０は、例えばパソコンのソフトウェアとして実現される、また、電子的商品としては、パソコン上で利用できるコンピュータソフトウェアやマルチメディアソフトウェアなどが考えられる。また販売会社６には、発注者から送られてくる発注情報を受け取る受付装置６０と、電子的商品を保管しておく商品保管部６１と、各発注者の識別子、パソコン通信アドレスおよび振替指定銀行口座等を保管しておく個人データ

10

格納部６２と、価格などの商品データを格納している商品データ格納部６３とが設けられている。

【０００５】発注者は、物品購入装置５０に欲しい電子的商品の商品コードＰＩＤを入力する。応じて、物品購入装置５０は、発注者の識別子ＵＩＤと商品コードＰＩＤを、パソコン通信を介して販売会社６に送信する。

【０００６】販売会社６では、受付装置６０が、発注者から送られてきた識別子ＵＩＤと商品コードＰＩＤとを受信する。次に、受付装置６０は、商品コードＰＩＤに対応する電子的商品ＰＤＴを商品保管部６０から取り出すと共に、商品データ格納部６３を検索して電子的商品ＰＩＤに対応する価格Ｐｒを求める。次に、受付装置６０は、送られてきた識別子ＵＩＤをもとに、個人データ格納部６２から、対応する発注者のパソコン通信アドレスと、振替指定銀行口座とを読み出す。次に、受付装置６０は、価格Ｐｒを発注者の振替指定銀行口座から販売会社の口座へ振り替えてもらうように、銀行に依頼する。次に、受付装置６０は、パソコン通信アドレスを参照して、発注者に発注を受けた商品ＰＤＴを送信する。

【０００７】発注者においては、物品発注装置５０が、発注した電子的商品ＰＤＴを受け取り、当該受け取った電子的商品ＰＤＴをパソコンなどのハードディスクに保存して使用する。

【０００８】なお、販売する商品が電子的商品でない場合にも、パソコン通信を用いて商品の発注を行い、販売会社は発注者の住所へ物理的な手段で発送することにより、商品の売買を行うことができる。

【０００９】【発明が解決しようとする課題】しかしながら、上記従来の通信販売システムでは、通信ネットワークを用いて商品の転送を行う必要性がある以上、通信の相手先を特定する必要がある。また、銀行振替やクレジットカードシステムなどの代金回収方法を用いようとすると、当然発注者を特定しなくてはならない。従って、販売会社に「誰が何を買ったか」という情報が伝わってしまうという特性がある。旧来の店頭での現金による物品販売では、発注者である購入者が名前を提示する必要がなく、販売店が「誰が買っているのか」は完全にはわからなかったことに比較し、上述の特性は通信ネットワークを用いた通信販売を実現するにあたって大きな問題点である。現在、各個人のプライバシの保護が大きく叫ばれており、この問題点は、通信ネットワークを用いた通信販売システムの普及に影響を及ぼすものと思われる。

【００１０】それゆえに、本発明の目的は、発注者が通信ネットワークを介して商品を注文購入する際に、発注者のプライバシ（例えば、「誰が何を買ったか」という情報）を確実に保護でき、しかもクレジットカードや銀行引き落しなどの既存の決裁システムをそのまま使用できる通信販売システムを提供することである。

【００１１】

11　　12

【課題を解決するための手段】請求項１に係る発明は、複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門および商品部門には、それぞれ、物品購入装置、受付装置および商品発送装置が設けられており、物品購入装置は、電子データから成る鍵を発生する鍵発生手段と、鍵を用いて、商品の発注内容を暗号化する発注内容暗号化手段と、鍵を暗号化する鍵暗号化手段と、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第１の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第１の受信手段と、第１の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第１の受信手段が受信した暗号化された商品の発注内容と暗号化された鍵とに、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する第２の送信手段と、発注者の識別情報と仮名情報との対応関係を記憶する対応関係記憶手段とを含み、商品発送装置は、受付装置から送信されてくるデータを受信する第２の受信手段と、第２の受信手段が受信した暗号化された鍵を復号する鍵復号手段と、復号された鍵を用いて、第２の受信手段が受信した暗号化された商品の発注内容を復号する発注内容復号手段と、電子的商品を保管する商品保管手段と、復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された鍵を用いて暗号化する商品暗号化手段と、暗号化された電子的商品を、第２の受信手段が受信した仮名情報と共に、受付装置に送信する第３の送信手段とを含み、受付装置は、さらに商品発送装置から送信されてくるデータを受信する第３の受信手段と、第３の受信手段が受信した仮名情報に基づいて、対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第３の受信手段が受信した暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第４の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【００１２】請求項２に係る発明は、請求項１の発明において、仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【００１３】請求項３に係る発明は、複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門、中継部門および商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、物品購入装置は、電子データから成る第１および第２の鍵を発生する鍵発生手段と、第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化手段と、第１および第２の鍵と、それぞれ別個に暗号化する鍵暗号化手段と、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第１の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第１の受信手段と、第１の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第１の受信手段が受信した２重に暗号化された商品の発注内容と暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、中継装置に送信する第２の送信手段と、発注者の識別情報と第１の仮名情報との対応関係を記憶する第１の対応関係記憶手段とを含み、中継装置は、受付装置から送信されてくるデータを受信する第２の受信手段と、第２の受信手段が受信した暗号化された第１の鍵を復号する第１の鍵復号手段と、復号された第１の鍵を用いて、第２の受信手段が受信した２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号手段と、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、商品発送装置に送信する第３の送信手段と、第１の仮名情報と第２の仮名情報との対応関係を記憶する第２の対応関係記憶手段とを含み、商品発送装置は、中継装置から送信されてくるデータを受信する第３の受信手段と、第３の受信手段が受信した暗号化された第２の鍵を復号する第２の鍵復号手段と、復号された第２の鍵を用いて、第３の受信手段が受信した部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号手段と、電子的商品を保管する商品保管手段と、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された第２の鍵を用いて暗号化する第１の商品暗号化手段と、第２の鍵を用いて暗号化された電子的商品を、第３の受信手段が受信した第２の仮名情報と共に、中継装置に送信する第４の送信手段とを含み、中継装置は、さらに商品発送装置から送信されてくるデータを受信する第４の受信手段と、第４の受信手段が受信した暗号化された電子的商品を、対応する第１の鍵を用いて２重に暗号化する第２の商品暗号化手段と、第４の受信手段が受信した第２の仮名情報に基づいて、第２の対応関係記憶手段を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する仮名情報特定手段と、第２の鍵を用いて２重に暗号化された電子的商品を、仮名情報特定手段により特定された第１の仮名情報と共に、受付装置に送信する第５の送信手段とを含み、受付装置は、さ

13　　14

らに中継装置から送信されてくるデータを受信する第５の受信手段と、第５の受信手段が受信した第１の仮名情報に基づいて、第１の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第５の受信手段が受信した２重に暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第６の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【００１４】請求項４に係る発明は、請求項３の発明において、第１および第２の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【００１５】請求項５に係る発明は、複数の発注者、受付部門、ｎ個（ｎは２以上の整数）の中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門、中継部門および商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、物品購入装置は、電子データから成る第１および第２の鍵を発生する鍵発生手段と、第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化手段と、第１および第２の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第１の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第１の受信手段と、第１の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第１の受信手段が受信した２重に暗号化された商品の発注内容と、暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、第１番目の中継部門に属する中継装置に送信する第２の送信手段と、発注者の識別情報と第１の仮名情報との対応関係を記憶する第１の対応関係記憶手段とを含み、第１番目の中継部門に属する中継装置は、受付装置から送信されてくるデータを受信する第２の受信手段と、第２の受信手段が受信した暗号化された第１の鍵を復号する第１の鍵復号手段と、復号された第１の鍵を用いて、第２の受信手段が受信した２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号手段と、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、第２番目の中継装置に属する中継装置に送信する第３の送信手段と、第１の仮名情報と第２の仮名情報との対応関係を記憶する第２の対応関係記憶手段とを含み、第ｍ番目（ｍは、２≦ｍ≦ｎ－１の整数）の中継部門に属する中継装置は、第（ｍ－１）番目の中継部門に属する中継装置から送信されてくるデータを受信する第３の受信手段と、第３の受信手段が受信した部分的に復号された商品の発注内容に、第ｍの仮名情報とは異なる第（ｍ＋１）の仮名情報を付加して、第（ｍ－１）番目の中継部門に属する中継装置に送信する第４の送信手段と、第ｍの仮名情報と第（ｍ－１）の仮名情報との対応関係を記憶する第３の対応関係記憶手段とを含み、第１番目の中継部門に属する中継装置は、第（ｎ－１）番目の中継部門に属する中継装置から送信されてくるデータを受信する第４の受信手段と、第４の受信手段が受信した部分的に復号された商品の発注内容に、第ｎの仮名情報とは異なる第（ｎ＋１）の仮名情報を付加して、商品発送装置に送信する第５の送信手段と、第ｎの仮名情報と第（ｎ＋１）の仮名情報との対応関係を記憶する第４の対応関係記憶手段とを含み、商品発送装置は、第ｎ番目の中継部門に属する中継装置から送信されてくるデータを受信する第５の受信手段と、第５の受信手段が受信した暗号化された第２の鍵を復号する第２の鍵復号手段と、復号された第２の鍵を用いて、第５の受信手段が受信した部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号手段と、電子的商品を保管する商品保管手段と、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された第２の鍵を用いて暗号化する第１の商品暗号化手段と、第２の鍵を用いて暗号化された電子的商品を、第５の受信手段が受信した第（ｎ＋１）の仮名情報と共に、第ｎ番目の中継部門に属する中継装置に送信する第６の送信手段とを含み、第ｎ番目の中継部門に属する中継装置は、さらに商品発送装置から送信されてくるデータを受信する第６の受信手段と、第６の受信手段が受信した第（ｎ－１）の仮名情報に基づいて、第４の対応関係記憶手段を検索し、当該第（ｎ＋１）の仮名情報に対応する第ｎの仮名情報を特定する第１の仮名情報特定手段と、第６の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第ｎの仮名情報と共に、第ｍ番目の中継部門に属する中継装置に送信する第７の送信手段とを含み、第ｍ番目の中継部門に属する中継装置は、さらに第（ｍ＋１）番目の中継部門に属する中継装置から送信されてくるデータを受信する第７の受信手段と、第７の受信手段が受信した第ｍの仮名情報に基づいて、第３の対応関係記憶手段を検索し、当該第ｍの仮名情報に対応する第（ｍ－１）の仮名情報を特定する第２の仮名情報特定手段と、第７の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第（ｍ－１）の仮名情報と共に、第（ｍ－１）番目の中継部門に属する中継装置に送信する第８の送信手段とを含み、第１番目の中継部門に属する中継装置は、さらに第２番目の中継部門に属する中継装置から送信されてくるデータを受信する第８の受信手段と、第８の受信手段が受信した暗

号化された電子的商品を、対応する第１の暗号鍵を用いて２重に暗号化する第２の商品暗号化手段と、第８の受信手段が受信した第２の仮名情報に基づいて、第３の対応関係記憶手段を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する第３の仮名情報特定手段と、第８の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第１の仮名情報と共に、受付装置に送信する第９の送信手段とを含み、受付装置は、さらに第１番目の中継部門に属する中継装置から送信されてくるデータを受信する第９の受信手段と、第９の受信手段が受信した第１の仮名情報に基づいて、第１の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第９の受信手段が受信した２重に暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第６の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【００１６】請求項６に係る発明は、複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、発注者においては、電子データから成る鍵を発生する鍵発生ステップと、鍵を用いて、商品の発注内容を暗号化する発注内容暗号化ステップと、鍵を暗号化する鍵暗号化ステップと、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第１の送信ステップとを実行し、受付部門においては、発注者から送信されてくるデータを受信する第１の受信ステップと、第１の受信ステップで受信した本人確認情報が、正当なものか否かを確認する確認ステップと、確認ステップによって本人確認情報が正当なものと確認された場合、第１の受信ステップで受信した暗号化された商品の発注内容と暗号化された鍵とに、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する第２の送信ステップと、発注者の識別情報と仮名情報との対応関係を記憶する対応関係記憶ステップとを実行し、商品部門においては、受付部門から送信されてくるデータを受信する第２の受信ステップと、第２の受信ステップで受信した暗号化された鍵を復号する鍵復号ステップと、復号された鍵を用いて、第２の受信ステップで受信した暗号化された商品の発注内容を復号する発注内容復号ステップと、復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が受付部門におわらないように梱包封印する梱包封印ステップと、梱包封印された商品を、第２の受信ステップで受信した仮名情報と共に、受付部門に発送する第１の発送ステップとを実行し、受付部門においては、さらに商品部門から受け取った仮名情報に基づいて、対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、商品部門から受け取った梱包封印された商品を、発注者特定ステップで特定された発注者に発送する第２の発送ステップとを実行することを特徴とする。

【００１７】請求項７に係る発明は、請求項６の発明において、仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【００１８】請求項８に係る発明は、複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、発注者においては、電子データから成る第１および第２の鍵を発生する鍵発生ステップと、第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する発注内容暗号化ステップと、第１および第２の鍵を、それぞれ別個に暗号化する鍵暗号化ステップと、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第１の送信ステップとを含み、受付部門においては、物品購入装置から送信されてくるデータを受信する第１の受信ステップと、第１の受信ステップで受信した本人確認情報が、正当なものか否かを確認する確認ステップと、確認ステップによって本人確認情報が正当なものと確認された場合、第１の受信ステップで受信した２重に暗号化された商品の発注内容と暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、中継装置に送信する第２の送信ステップと、発注者の識別情報と第１の仮名情報との対応関係を記憶する第１の対応関係記憶ステップとを実行し、中継部門においては、受付装置から送信されてくるデータを受信する第２の受信ステップと、第２の受信ステップで受信した暗号化された第１の鍵を復号する第１の鍵復号ステップと、復号された第１の鍵を用いて、第２の受信ステップで受信した２重に暗号化された商品の発注内容を、部分的に復号する第１の発注内容復号ステップと、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、商品発送装置に送信する第３の送信ステップと、第１の仮名情報と第２の仮名情報との対応関係を記憶する第２の対応関係記憶ステップとを実行し、商品部門においては、中継装置から送信されてくるデータを受信する第３の受信ステップと、第３の受信ステップで受信した暗号化された第２の鍵を復号する第２の鍵復号ステップと、復号された第２の鍵を用いて、第３の受信ステップで受信した部分的に復号された商品の発注内容を全面的に復号する第２の発注内容復号ステップと、全面的に復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が受付部門におわらないように梱包封印する第１の梱包封印ステップと、梱包封印された商品を、第２の受信ステップで受信した仮名情報と共に、中継部門に発送する第１の発送ステップとを実行し、中継部門においては、さらに商品部門から受け取っ

た梱包封印された商品を、さらに２重に梱包封印する第２の梱包封印ステップと、商品部門から受け取った第２の仮名情報に基づいて、第２の対応関係記憶ステップで記憶した対応関係を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する仮名情報特定ステップと、２重に梱包封印された商品を、仮名情報特定ステップにより特定された第１の仮名情報と共に、受付部門に発送する第２の発送ステップとを実行し、受付部門においては、さらに中継部門から受け取った第１の仮名情報に基づいて、第１の対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、中継部門から受け取った２重に梱包封印された商品を、発注者特定ステップにより特定された発注者に発送する第３の発送ステップとを実行することを特徴とする。

【００１９】請求項９に係る発明は、請求項８の発明において、第１および第２の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【００２０】

【作用】請求項１に係る発明においては、発注者、受付部門および商品部門は、相互に通信ネットワークで結ばれており、物品購入装置、受付装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る鍵を発生し、当該鍵を用いて商品の発注内容を暗号化する。また、当該鍵を暗号化する。さらに、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した発注内容および暗号化された鍵に、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する。また、発注者の識別情報と仮名情報との対応関係を対応関係記憶手段に記憶する。商品発送装置は、受付装置から受信した暗号化された鍵を復号し、当該復号された鍵を用いて、受付装置から受信した暗号化された商品の発注内容を復号する。また、復号された商品の発注内容に基づいて、対応する電子的商品を商品保管手段から読み出し、この読み出した電子的商品を、復号された鍵を用いて暗号化し、仮名情報と共に、受付装置に送信する。受付装置は、さらに商品発送装置から受信した仮名情報に基づいて、対応関係記憶手段を検索し、対応する発注者を特定する。そして、暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する。

【００２１】請求項２に係る発明においては、仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

【００２２】請求項３に係る発明においては、発注者、受付部門、中継部門および商品部門は、相互に通信ネットワークで結ばれており、物品購入装置、受付装置、中継装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る第１および第２の鍵を発生し、当該第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する。また、第１および第２の鍵を、それぞれ別個に暗号化する。さらに、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した２重に暗号化された商品の発注内容と暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、中継装置に送信する。また、発注者の識別情報と第１の仮名情報との対応関係を第１の対応関係記憶手段に記憶する。中継装置は、受付装置から受信した暗号化された第１の鍵を復号し、この復号された第１の鍵を用いて、受付装置から受信した２重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、商品発送装置に送信する。さらに、第１の仮名情報と第２の仮名情報との対応関係を第２の対応関係記憶手段に記憶する。商品発送装置は、中継装置から受信した暗号化された第２の鍵を復号し、この復号された第２の鍵を用いて、中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出し、この読み出した電子的商品を、復号された第２の鍵を用いて暗号化する。さらに、第２の鍵を用いて暗号化された電子的商品を、第３の受信手段が受信した第２の仮名情報と共に、中継装置に送信する。中継装置は、さらに商品発送装置から受信した暗号化された電子的商品を、対応する第１の鍵を用いて２重に暗号化する。また、商品発送装置から受信した第２の仮名情報に基づいて、第２の対応関係記憶手段を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する。さらに、２重に暗号化された電子的商品を、特定された第１の仮名情報と共に、受付装置に送信する。受付装置は、さらに中継装置から受信した第１の仮名情報に基づいて、第１の対応関係記憶手段を検索し、対応する発注者を特定する。また、中継装置から受信した２重に暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する。

【００２３】請求項４に係る発明においては、第１および第２の仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

19

【００２４】請求項５に係る発明においては、複数の発注者、受付部門、ｎ個（ｎは２以上の整数）の中継部門、商品部門は、通信ネットワークを用いて相互に結ばれており、物品購入装置、受付装置、中継装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る第１および第２の鍵を発生し、この第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する。また、第１および第２の鍵を、それぞれ別個に暗号化する。さらに、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した２重に暗号化された商品の発注内容と、暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、第１番目の中継部門に属する中継装置に送信する。また、発注者の識別情報と第１の仮名情報との対応関係を第１の対応関係記憶手段に記憶する。第１番目の中継部門に属する中継装置は、受付装置から受信した暗号化された第１の鍵を復号し、この復号された第１の鍵を用いて、受付装置から受信した２重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、第２番目の中継装置に属する中継装置に送信する。さらに、第１の仮名情報と第２の仮名情報との対応関係を第２の対応関係記憶手段に記憶する。第ｍ番目（ｍは、２≦ｍ≦ｎ－１の整数）の中継部門に属する中継装置は、第（ｍ－１）番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容に、第ｍの仮名情報とは異なる第（ｍ＋１）の仮名情報を付加して、第（ｍ＋１）番目の中継部門に属する中継装置に送信する。また、第ｍの仮名情報と第（ｍ＋１）の仮名情報との対応関係を第３の対応関係記憶手段に記憶する。第ｎ番目の中継部門に属する中継装置は、第（ｎ－１）番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容に、第ｎの仮名情報とは異なる第（ｎ＋１）の仮名情報を付加して、商品発送装置に送信する。また、第ｎの仮名情報と第（ｎ＋１）の仮名情報との対応関係を第４の対応関係記憶手段に記憶する。商品発送装置は、第ｎ番目の中継部門に属する中継装置から受信した暗号化された第２の鍵を復号し、この復号された第２の鍵を用いて、第ｎ番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、商品保管手段から対応する電子的商品を読み出し、この読み出した電子的商品を、復号された第２の鍵を用いて暗号化する。さらに、第２の鍵を用いて暗号化された電子的商品を、第ｎ番目の中継部門に属する中継装置から受

20

信した第（ｎ－１）の仮名情報と共に、第ｎ番目の中継部門に属する中継装置に送信する。第ｎ番目の中継部門に属する中継装置は、さらに商品発送装置から受信した第（ｎ－１）の仮名情報に基づいて、第４の対応関係記憶手段を検索し、当該第（ｎ＋１）の仮名情報に対応する第ｎの仮名情報を特定する。また、商品発送装置から受信した暗号化された電子的商品を、特定された第ｎの仮名情報と共に、第ｍ番目の中継部門に属する中継装置に送信する。第ｍ番目の中継部門に属する中継装置は、さらに第（ｍ＋１）番目の中継部門に属する中継装置から受信した第ｍの仮名情報に基づいて、第３の対応関係記憶手段を検索し、当該第ｍの仮名情報に対応する第（ｍ－１）の仮名情報を特定する。また、第（ｍ－１）番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、特定された第（ｍ－１）の仮名情報と共に、第（ｍ－１）番目の中継部門に属する中継装置に送信する。第１番目の中継部門に属する中継装置は、さらに第２番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、対応する第１の暗号鍵を用いて２重に暗号化する。また、第２番目の中継部門に属する中継装置から受信した第２の仮名情報に基づいて、第３の対応関係記憶手段を検索し、当該第２の仮名情報に対応する第１の仮名情報を特定する。さらに、第２番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、特定された第１の仮名情報と共に、受付装置に送信する。受付装置は、さらに第１番目の中継部門に属する中継装置から受信した第１の仮名情報に基づいて、第１の対応関係記憶手段を検索することにより、対応する発注者を特定する。また、第１番目の中継部門に属する中継装置から受信した２重に暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を受信する。

【００２５】請求項６に係る発明においては、複数の発注者、受付部門、商品部門が、通信ネットワークを用いて互いに結ばれており、これらの間で実体的商品の発注と流通を行う。すなわち、発注者は、電子データから成る鍵を発生し、この鍵を用いて、商品の発注内容を暗号化する。また、鍵を暗号化する。さらに、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付部門は、発注者から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、発注者から受信した暗号化された商品の発注内容と暗号化された鍵とに、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する。また、発注者の識別情報と仮名情報との対応関係を記憶する。商品部門は、受付部門から受信した暗号化された鍵を復号し、この復号された鍵を用いて、受付部門から受信した暗号化された商品の発注内容を復号する。また、復号された商品の発注

21　　22

内容に基づいて、対応する商品を特定し、その内容が受付部門におかならないように梱包封印する。さらに、梱包封印された商品を、第２の受信ステップで受信した仮名情報と共に、受付部門に発送する。受付部門は、さらに商品部門から受け取った仮名情報に基づいて、対応する発注者を特定し、商品部門から受け取った梱包封印された商品を、特定された発注者に発送する。

【００２６】請求項７に係る発明においては、仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

【００２７】請求項８に係る発明においては、複数の発注者、受付部門、中継部門、商品部門が、通信ネットワークを用いて互いに結ばれており、これらの間で実体的商品の発注と流通を行う。すなわち、発注者は、電子データから成る第１および第２の鍵を発生し、この第１および第２の鍵を用いて、商品の発注内容を２重に暗号化する。また、第１および第２の鍵を、それぞれ別個に暗号化する。さらに、２重に暗号化された商品の発注内容に、暗号化された第１および第２の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付部門は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した２重に暗号化された商品の発注内容と暗号化された第１および第２の鍵とに、発注者の識別情報とは異なる第１の仮名情報を付加して、中継装置に送信する。また、発注者の識別情報と第１の仮名情報との対応関係を第１の対応関係記憶手段に記憶する。中継部門は、受付装置から受信した暗号化された第１の鍵を復号し、この復号された第１の鍵を用いて、受付装置から受信した２重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報を付加して、商品発送装置に送信する。さらに、第１の仮名情報と第２の仮名情報との対応関係を第２の対応関係記憶手段に記憶する。商品部門は、中継装置から受信した暗号化された第２の鍵を復号し、この復号された第２の鍵を用いて、中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が受付部門におかならないように梱包封印する。さらに、梱包封印された商品を、中継装置から受信した仮名情報と共に、中継部門に発送する。中継部門は、さらに商品部門から受け取った梱包封印された商品を、さらに２重に梱包封印する。また、商品部門から受け取った第２の仮名情報に基づいて、対応する第１の仮名情報を特定し、２重に梱包封印された商品を、この特定された第１の仮名情報と共に、受付部門に発送する。

受付部門は、さらに中継部門から受け取った第１の仮名情報に基づいて、対応する発注者を特定し、中継部門から受け取った２重に梱包封印された商品を、この特定された発注者に発送する。

【００２８】請求項９に係る発明においては、第１および第２の仮名情報として、各注文毎に異なる情報が使用することにより、プライバシーの機密性をより一層向上させている。

【００２９】

【実施例】図１は、本発明の一実施例に係る通信ネットワークを用いた通信販売システムの構成を示すブロック図である。図１において、本実施例のネットワークを用いた通信販売システムは、複数の発注者ｉと販売会社から成り立っている。販売会社は、受付部門ａ、中継部門ｂ、商品部門ｃとに分かれており、各部門は独立に業務を遂行しており、各部門間で情報の公開は無いものとする。また、本システムに加入している発注者ｉには、各個人を識別できる発注者識別子ＩＤｉが付与されている。また、本実施例の通信ネットワークを用いた通信販売システムは、商品として、ゲームや業務用のソフトウェア、マルチメディア情報などの電子的商品を取り扱うものとする。

【００３０】図１において、発注者ｉは、販売会社の受付部門ａとパソコン通信でつながっていて、双方向に情報をやりとりする。受付部門ａは、発注者ｉおよび中継部門ｂとパソコン通信でつながっていて、双方向に情報をやりとりする。中継部門ｂは、受付部門ａおよび商品部門ｃとパソコン通信でつながっていて、双方向に情報をやりとりする。商品部門ｃは、中継部門ｂとパソコン通信でつながっていて、双方向に情報をやりとりする。

【００３１】次に、図１に示す通信販売システムの概略的な動作を説明する。まず、発注者ｉは、欲しい商品の商品コードを２重に暗号化し、それを解読するための２つの暗号鍵をそれぞれ、中継部門ｂ、商品部門ｃ向けに暗号化する。そして、発注者ｉは、二重に暗号化された商品コードと、中継部門ｂおよび商品部門ｃ向けに暗号化した暗号鍵とを合わせた暗号化発注内容を、発注者の識別子と共に、販売会社の受付部門ａに送る。受付部門ａは、発注者ｉから送られてきた情報、すなわち暗号化発注内容を、そのまま、照会番号（仮名情報）Ｒｅｆ１と共に、中継部門ｂに送る。中継部門ｂは、受付部門ａから送られてきた暗号化発注内容の内、中継部門ｂ向けに暗号化された暗号鍵を復号し、それを用いて二重に暗号化されている商品コードを一部復号する。そして、中継装置ｂは、一部復号された暗号化された商品コードと、商品部門ｃ向けに暗号化された暗号鍵とを合わせて、照会番号Ｒｅｆ２と共に、商品部門ｃへ送る。商品部門ｃは、商品部門ｃ向けに暗号化された暗号鍵を復号し、当該復号された暗号鍵を用いて、暗号化されている商品コードを復号する。これによって、発注されている商品名を知ることができる。

【００３２】次に、商品部門ｃは、復号した商品コードに対応する商品そのものを暗号化し、当該暗号化された

商品を、その価格および照会番号Ｒｅｆ２と共に、中継部門ｂに送る。中継部門ｂは、商品部門ｃから送られてきた暗号化商品をさらに暗号化し、当該二重に暗号化された商品を、その価格および照会番号Ｒｅｆ１と共に、受付部門ａに送る。受付部門ａは、照会番号Ｒｅｆ１から発注者ｉを対応づけ、商品の価格に等しい金額を発注者ｉの銀行口座から引き落とし、また中継部門ｂから送られてきた暗号化商品を、通信ネットワークを介して発注者ｉに送る。発注者ｉは、受付部門ａから送られてきた暗号化商品を復号し、発注した商品を手に入れる。

【００３３】図２は、図１に示す発注者ｉが所持している物品購入装置１０の構成の一例を示すブロック図である。図２において、この物品購入装置１０は、制御部１０１と、ＲＯＭ１０２と、ＲＡＭ１０３と、入力操作器１０４と、表示器１０５と、商品カタログ格納部１０６と、乱数発生部１０７と、秘密鍵保管部１０８と、通信部１０９と、発注データ格納部１１０とを備えている。

【００３４】ＲＯＭ１０２には、プログラムデータと、受付部門ａの公開鍵、中継部門ｂの公開鍵、商品部門ｃの公開鍵が格納され、制御部１０１は、このプログラムデータに従って動作する。ＲＡＭ１０３は、制御部１０１の動作に必要な種々のデータを記憶する。入力操作器１０４は、発注者によって操作されるキーボードやマウス等を含み、制御部１０１に種々のデータや指示を入力する。表示器１０５は、ＣＲＴディスプレイや液晶表示器によって構成され、制御部１０１から与えられる画像データを表示する。商品カタログ格納部１０６は、受付部門ａから定期的に送られてくる電子的な画像データを含む商品カタログを格納する。乱数発生部１０７は、発注内容の暗号化に必要な２つの乱数を生成する。秘密鍵保管部１０８は、発注者ｉ固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部１０９は、受付部門ａとパソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部１１０は、商品発注データをやりとりする際に必要なデータを記憶している。

【００３５】図３は、図１に示す受付部門ａに設けられている受付装置２０の構成の一例を示すブロック図である。図３において、この受付装置２０は、制御部２０１と、ＲＯＭ２０２と、ＲＡＭ２０３と、個人データ格納部２０４と、秘密鍵保管部２０５と、通信部２０６と、発注データ格納部２０７と、照会番号発行部２０８とを備えている。

【００３６】ＲＯＭ２０２には、プログラムデータならびに中継部門ｂの公開鍵が格納され、制御部２０１は、このプログラムデータに従って動作する。ＲＡＭ２０３は、制御部２０１の動作に必要な種々のデータを記憶する。個人データ格納部２０４には、本システムに加入している全ユーザの公開鍵、パソコン通信アドレス、銀行口座などの個人情報が、個人識別子と組にされて保管されている。秘密鍵保管部２０５は、受付部門ａ固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部２０６は、各発注者および中継部門ｂと、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部２０７は、商品発注データをやりとりする際に必要なデータを記憶している。照会番号発行部２０８は、商品発注データのやりとりをする際に必要な照会番号を発行する。

【００３７】図４は、図１に示す中継部門ｂに設けられている中継装置３０の構成の一例を示すブロック図である。図４において、この受付装置３０は、制御部３０１と、ＲＯＭ３０２と、ＲＡＭ３０３と、秘密鍵保管部３０４と、通信部３０５と、発注データ格納部３０６と、照会番号発行部３０７とを備えている。

【００３８】ＲＯＭ３０２には、プログラムデータならびに受付部門ａの公開鍵が格納され、制御部３０１は、このプログラムデータに従って動作する。ＲＡＭ３０３は、制御部３０１の動作に必要な種々のデータを記憶する。秘密鍵保管部３０４は、受付部門ｂ固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部３０５は、受付部門ａと、商品部門ｃと、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部３０６は、商品発注データをやりとりする際に必要なデータを記憶している。照会番号発行部３０７は、商品発注データのやりとりをする際に必要な照会番号を発行する。

【００３９】図５は、図１に示す商品部門ｃに設けられた商品発送装置４０の構成の一例を示すブロック図である。図５において、この商品発送装置４０は、制御部４０１と、ＲＯＭ４０２と、ＲＡＭ４０３と、秘密鍵保管部４０４と、通信部４０５と、発注データ格納部４０６と、商品データ格納部４０７と、商品保管部４０８とを備えている。

【００４０】ＲＯＭ４０２には、プログラムデータならびに中継部門ｂの公開鍵が格納され、制御部４０１は、このプログラムデータに従って動作する。ＲＡＭ４０３は、制御部４０１の動作に必要な種々のデータを記憶する。秘密鍵保管部４０４は、受付部門ｃ固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部４０５は、中継部門ｂと、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部４０６は、商品発注データをやりとりをする際に必要なデータを記憶している。商品データ格納部４０７は、各商品の価格などが格納されている。商品保管部４０８は、商品部門ｃが販売する全電子的商品が記録されている。ただし外部から読み出すことはできない。

【００４１】図６は、図１に示す通信ネットワークを用いた通信販売システム全体の動作を示すシーケンスチャートである。図７は、図１の物品購入装置１０の商品発

25　　26

注時の動作を示すフローチャートである。図８は、図１の受付装置２０の発注受付時の動作を示すフローチャートである。図９は、図１の中継装置３０の発注中継時の動作を示すフローチャートである。図１０は、図１の商品発送装置４０の動作を示すフローチャートである。図１１は、図１の中継装置３０の商品中継時の動作を示すフローチャートである。図１２は、図１の受付装置２０の商品発送時の動作を示すフローチャートである。図１３は、図１の物品購入装置１０の商品受取時の動作を示すフローチャートである。以下、これら図６～１３を参照して、上記実施例の動作を説明する。

【００４２】各発注者ｉは、本システム加入時に、システム管理者に対して名前，パソコン通信アドレス，振替指定銀行口座などを書いたシステム加入申込書を送る。また同時に、振替指定銀行口座のある銀行に対して，銀行に受付部門ａから正当な料金振替請求があった場合には，銀行は発注者ｉの許可なしで振り替えできる、という内容の契約書を送っておく。システム管理者は、発注者ｉから送られてきたシステム加入申込書の内容の確認を行い、確認が取れた場合，発注者ｉに個人識別子ＩＤｉと、発注者毎に異なりかつ秘密にしておく必要のある秘密鍵などを格納した物品購入装置１０を配布（貸与、販売）する。また、システム管理者は，受付部門ａに，発注者ｉの個人識別子ＩＤｉと、公開鍵ｐｉと、振替指定口座とを組にして伝え、受付部門ａは、そのデータを図１の受付装置１０内にある個人データ格納部２０４（図３参照）に格納しておく。

【００４３】システム管理者は、各発注者ｉ、中継部門ｂ、商品部門ｃに対して、秘密鍵暗号アルゴリズムＦと秘密鍵復号アルゴリズムＦ－１を配布しておく。このとき、鍵Ｋを用いて秘密鍵暗号アルゴリズムＦによりデータＸを暗号化した関数Ｆ（Ｋ，Ｘ）を復号できるのは、秘密鍵復号アルゴリズムＦ－１と鍵Ｋの双方を保持しているものに限られる。すなわち、

Ｘ＝Ｆ－１（Ｋ，Ｆ（Ｋ，Ｘ））

が成立する。

【００４４】次に、システム管理者は、各発注者ｉに対して、公開鍵暗号アルゴリズムＥと、中継部門ｂおよび商品部門ｃの公開鍵ｐｂおよびｐｃとを配布し、中継部門ｂおよび商品部門ｃに対して、公開鍵復号アルゴリズムＤと、各自の秘密鍵ｓｂおよびｓｃとを配布する（公開鍵，秘密鍵は、商品部門毎に異なる）。このとき、ｙ（ｙは、ｂかｃのいずれか）の公開鍵ｐｙを用いて公開鍵暗号アルゴリズムＥによりデータＸを暗号化した関数Ｅ（ｐｙ，Ｘ）を復号できるのは，公開鍵復号アルゴリズムＤと秘密鍵ｓｙを保持しているものに限られる。すなわち、

Ｘ＝Ｄ（ｓｙ，Ｅ（ｐｙ，Ｘ））

が成立する。また、秘密鍵ｓｙは、ｙしか知らない。また、各公開鍵ｐｙから対応する秘密鍵ｓｙは類推できない。

【００４５】また、システム管理者は、各発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃに対して、署名生成アルゴリズムｓｉｇｎおよび署名確認アルゴリズムｖｅｒｉｆｙと、受付部門ａ，中継部門ｂ，商品部門ｃの公開鍵とを配布する（先に公開鍵暗号アルゴリズムの説明の時に述べた公開鍵・秘密鍵の値と同じである）。このとき、データＸに対して自分の秘密鍵ｓｙ（ｙは、ｉ、ａ、ｂ、ｃのいずれか）を用いて署名生成アルゴリズムｓｉｇｎにより作成した電子署名ｓｉｇｎ（ｓｙ，Ｘ）は、秘密鍵ｓｙを保持していないと作成できない。また、ｙの公開鍵ｐｙと署名確認アルゴリズムｖｅｒｉｆｙとを用いることにより、電子署名ｓｉｇｎ（ｓｙ，Ｘ）が、確かにｙの作成したデータＸに対する電子署名であるか否かを確認できる。

【００４６】各発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃにおいては、配布されたアルゴリズムと各公開鍵とが、各装置の内部にあるＲＯＭ１０２、２０２、３０２、４０２にそれぞれ格納してある。また、各自の秘密鍵は、各装置内部の秘密鍵保管部１０８、２０５、３０４、４０４に保管され、外部からは読み出しできない。

【００４７】なお、秘密鍵暗号アルゴリズム、公開鍵暗号アルゴリズム、署名生成アルゴリズムに関しては、「現代暗号理論」池野信一・小山謙二著（電子通信学会）に詳しく述べられているので、それを参照されたい。

【００４８】以下の処理は、ある発注者ｉが、商品コードＰＩＤの電子的商品ＰＤＴを購入する場合の処理について述べている。

【００４９】発注者ｉには、定期的に受付部門ａから電子カタログが送付されてきて、商品カタログ格納部１０６に格納されている。発注者ｉは、商品カタログ格納部１０６に格納されている電子カタログが、表示器１０５に表示されるのを見て、欲しいと思った商品があった場合、入力操作器１０４で画面をマークすることにより、購入商品を選択してその結果を制御部１０１に入力する（図７のステップＳ１０１）。なお、購入商品の選択方法には、これ以外にも種々の方法（例えば、キー入力）を取り得ることを指摘しておく。次に、制御部Ｊ１０１は、入力された購入商品に対応する商品コードＰＩＤを、商品カタログ格納部１０６から読みとる（ステップＳ１０２）。

【００５０】次に、制御部１０１は、乱数発生部１０７を用いて２つの乱数ｒｂ，ｒｃを発生する（ステップＳ１０３）。次に、制御部１０１は、ＲＯＭ１０２から秘密鍵暗号アルゴリズムＦを読み込み、発生された乱数ｒｂ，ｒｃを鍵として、商品コードＰＩＤを次のように二重暗号化する（ステップＳ１０４）。まず、ｒｃを鍵としてＰＩＤを暗号化する。

27　　28

F（r c，P I D）

さらに、上記データF（r c，P I D）を、r bを鍵として暗号化する。

F（r b，F（r c，P I D））

【0051】次に、制御部101は、ROM102から、公開鍵暗号アルゴリズムEと、中継部門bの公開鍵p bと、購入しようとしている商品を販売する商品部門cの公開鍵p cとを読み込み、下式（1）のように乱数r bを公開鍵p bを用いて公開鍵暗号アルゴリズムEにより暗号化し、下式（2）のように乱数r cを公開鍵p cを用いて公開鍵暗号アルゴリズムEにより暗号化する（ステップS105）。

E（p b，r b）　…（1）

E（p c，r c）　…（2）

【0052】次に、制御部101は、F（r b，F（r c，P I D））、E（p b，r b）、E（p c，r c）を連結して、下式（3）のように、暗号化発注内容EOr d1を生成する（ステップS106）。

EOr d1＝F（r b，F（r c，P I D））‖E（p b，r b）‖E（p c，r c）　…（3）

ただし、上式（3）において、‖は情報の連結を表している。

【0053】次に、制御部101は、秘密鍵保管部108から発注者iの秘密鍵s iを、そしてROM102から署名生成アルゴリズムs i g nを、それぞれ読み取り、下式（4）を用いて、EOr d1に対する電子署名を生成する（ステップS107）。

s i g n（s i，EOr d1）　…（4）

ここで、データXと、データXに対するyの電子署名s i g n（s y，X）の連結を、X［y］で簡単に表すことにする。すなわち、

X［y］＝X‖s i g n（s y，X）

となる。

【0054】次に、制御部101は、個人識別子I DiとEOr d1［i］とを、通信部109からパソコン通信を用いて、受付部門aに送信する（ステップS108）。

【0055】受付部門aは、パソコン通信を用いて発注者iから送られてきたデータI DiとEOr d1［i］とを、図3の通信部206を介して受信する（図8のステップS201）。次に、受付装置20の制御部201は、送られてきたデータのI Diから対応する公開鍵p iを、個人データ格納部204から検索して、読み出す（ステップS202）。次に、制御部201は、ROM202から署名確認アルゴリズムv e r i f yを読み出し、EOr d1［i］の電子署名s i g n（s i，EOr d1）がEOr d1に対する発注者iの電子署名であるか否かを、下式（5）を用いて確認する（ステップS203）。

v e r i f y（p i，s i g n（s i，EOr d1））　…（5）

制御部201は、電子署名の正当性が確認できれば、ステップS204へ進み、確認できない場合は、署名の正当性が確認できなかった旨を、通信部206を介して発注者iへ伝える（ステップS205）。

【0056】次に、制御部201は、照会番号発行部208を用いて照会番号R e f 1を発行する（ステップS204）。次に、制御部201は、R e f 1，I Di，EOr d1［i］を組にして、発注データ格納部207に格納する（ステップS206）。次に、制御部201は、ROM202から署名生成アルゴリズムs i g nを、そして秘密鍵保管部205から秘密鍵s aを、それぞれ読み出し、次式（6）を用いて、照会番号R e f 1に対する電子署名を生成する（ステップS207）。

s i g n（s a，R e f 1）　…（6）

【0057】次に、制御部201は、R e f 1［a］を受付番号として、発注者iに、通信部206からパソコン通信を用いて送信する（ステップS208）。

【0058】発注者iは、受付部門aから送られてきたR e f 1［a］と、暗号化発注内容EOr d1と、2つの乱数r b，r cとを組にして、発注データ格納部11より暗号化し、下式（2）のように乱数r cを公開鍵p cを用いて公開鍵暗号アルゴリズムEにより暗号化する（ステップS105）。

E（p b，r b）　…（1）

E（p c，r c）　…（2）

【0052】次に、制御部101は、F（r b，F（r c，P I D））、E（p b，r b）、E（p c，r c）を連結して、下式（3）のように、暗号化発注内容EOr d1を生成する（ステップS106）。

EOr d1＝F（r b，F（r c，P I D））‖E（p b，r b）‖E（p c，r c）　…（3）

ただし、上式（3）において、‖は情報の連結を表している。

【0053】次に、制御部101は、秘密鍵保管部108から発注者iの秘密鍵s iを、そしてROM102から署名生成アルゴリズムs i g nを、それぞれ読み取り、下式（4）を用いて、EOr d1に対する電子署名を生成する（ステップS107）。

s i g n（s i，EOr d1）　…（4）

ここで、データXと、データXに対するyの電子署名s i g n（s y，X）の連結を、X［y］で簡単に表すことにする。すなわち、

X［y］＝X‖s i g n（s y，X）

となる。

【0054】次に、制御部101は、個人識別子I DiとEOr d1［i］とを、通信部109からパソコン通信を用いて、受付部門aに送信する（ステップS108）。

【0055】受付部門aは、パソコン通信を用いて発注者iから送られてきたデータI DiとEOr d1［i］とを、図3の通信部206を介して受信する（図8のステップS201）。次に、受付装置20の制御部201は、送られてきたデータのI Diから対応する公開鍵p iを、個人データ格納部204から検索して、読み出す（ステップS202）。次に、制御部201は、ROM202から署名確認アルゴリズムv e r i f yを読み出し、EOr d1［i］の電子署名s i g n（s i，EOr d1）がEOr d1に対する発注者iの電子署名であるか否かを、下式（5）を用いて確認する（ステップS203）。

v e r i f y（p i，s i g n（s i，EOr d1））　…（5）

制御部201は、電子署名の正当性が確認できれば、ステップS204へ進み、確認できない場合は、署名の正当性が確認できなかった旨を、通信部206を介して発注者iへ伝える（ステップS205）。

【0056】次に、制御部201は、照会番号発行部208を用いて照会番号R e f 1を発行する（ステップS204）。次に、制御部201は、R e f 1，I Di，EOr d1［i］を組にして、発注データ格納部207に格納する（ステップS206）。次に、制御部201は、ROM202から署名生成アルゴリズムs i g nを、そして秘密鍵保管部205から秘密鍵s aを、それぞれ読み出し、次式（6）を用いて、照会番号R e f 1に対する電子署名を生成する（ステップS207）。

s i g n（s a，R e f 1）　…（6）

【0057】次に、制御部201は、R e f 1［a］を受付番号として、発注者iに、通信部206からパソコン通信を用いて送信する（ステップS208）。

【0058】発注者iは、受付部門aから送られてきたR e f 1［a］と、暗号化発注内容EOr d1と、2つの乱数r b，r cとを組にして、発注データ格納部11

v e r i f y（p a，s i g n（s a，R e f 1‖EOr d1））…（8）

5を介して受付部門aへ署名の正当性が確認できなかった旨を伝える（ステップS304）。

制御部301は、電子署名の正当性が確認できればステップS303へ進み、確認できない場合は、通信部30

29

【0061】次に、制御部301は、EOrd1からE（pb，rb）を取り出し、秘密鍵保管部304から秘密鍵sbを、そしてROM302から公開鍵復号アルゴリズムDを読み込み、次式（9）に示すように、E（pb，rb）を鍵sbを用いてDにより復号し、rbを得る（ステップS303）。

D（sb，E（pb，rb））＝rb　…（9）

次に、制御部301は、ROM302から秘密鍵復号アルゴリズムF⁻¹を読み出し、次式（10）に示すようにEOrd1のF（rb，F（rc，PID））をrbを用いて一部だけ復号する（ステップS305）。

F⁻¹（rb，F（rb，F（rc，PID））；

＝F（rc，PID）　…（10）

【0062】次に、制御部301は、F（rc，PID）とEOrd1のE（pc，rc）とを連結して、次式（11）で示されるEOrd2を生成する（ステップS306）。

EOrd2＝F（rc，PID）｜E（pc，rc）　…（11）

【0063】次に、制御部301は、照会番号登行部307を用いて、照会番号Ref2を発行する（ステップS307）。次に、制御部301は、（Ref1｜EOrd1）［a］と、照会番号Ref2とを組にして、発注データ格納部306に格納する（ステップS308）。

sign（sb，Ref2｜EOrd2）　…（12）

【0064】次に、制御部301は、（Ref2｜EOrd2）［b］を、商品部門cに、通信部305からパソコン通信を用いて送信する（ステップS310）。

【0065】商品部門cは、パソコン通信を用いて中継部門bから送られてきたデータ（Ref2｜EOrd2）［b］を、図5の通信部405を介して受信する（図10のステップS401）。商品発送装置40の制御部401は、電子署名の正当性が確認できればステップS403へ進み、確認できない場合は、通信部405を介して中継部門bへ署名の正当性が確認できなかった旨を伝える（ステップS404）。

【0066】次に、制御部401は、EOrd2からE（pc，rc）を取り出し、秘密鍵保管部404から秘密鍵scを、そしてROM402から公開鍵復号アルゴリズムDを読み込み、E（pc，rc）を鍵scを用いてDにより復号し、次式（13）で示されるrcを得る（ステップS403）。

verify（pb，sign（sb，Ref2｜EOrd2））　…（13）

D（sc，E（pc，rc））＝rc　…（14）

次に、制御部401は、ROM402から秘密鍵復号アルゴリズムF⁻¹を読み出し、EOrd2のF（rc，PID）をrcだけを用いて次式（15）のように復号する（ステップS405）。

F⁻¹（rc，F（rc，PID））＝PID　…（15）

次に、制御部401は、（Ref2｜EOrd2）［b］を、発注データ格納部406に格納する（ステップS406）。

【0067】次に、制御部401は、PIDの価格Prを商品データ格納部406から読み出し（ステップS407）、商品保管部408からPIDが対応する電子的商品PDTを取り出す（ステップS408）。次に、制御部401は、ROM402から秘密鍵暗号アルゴリズムFを読み込み、PDTを鍵rcを用いてFにより暗号化することにより、次式（16）で示されるEPDT1を生成する（ステップS409）。

EPDT1＝F（rc，PDT）　…（16）

【0068】次に、制御部401は、ROM402から署名生成アルゴリズムsignを読み込み、Ref2、EDPT1、Prを連結したものに対して、次式（17）で示されるような電子署名を作成する（ステップS410）。

sign（sc，Ref2｜EDPT1｜Pr）　…（17）

【0069】次に、制御部401は、（Ref2｜EDPT1｜Pr）［c］を、中継部門bに、通信部405からパソコン通信を用いて送信する（ステップS411）。

【0070】中継部門bは、パソコン通信を用いて商品部門cから送られて来たデータ（Ref2｜EDPT1｜Pr）［c］を、図4の通信部304を介して受信する（図11のステップS501）。中継装置30の制御部301は、ROM302から、署名確認アルゴリズムverifyと、商品部門cの公開鍵pcとを読み出し、（Ref2｜EDPT1｜Pr）［c］の電子署名sign（sc，Ref2｜EDPT1｜Pr）が、御部401は、ROM402から、署名確認アルゴリズムverifyと、中継部門bの公開鍵pbとを読み出し、（Ref2｜EOrd2）［b］の電子署名sign（sb，Ref2｜EOrd2）が、（Ref2｜EOrd2）に対する中継部門bの電子署名であるか否かを、次式（13）を用いて確認する（ステップS402）。

（Ｒｅｆ２‖ＥＤＰＴ１‖Ｐｒ）に対する商品部門ｃの電子署名であるか否かを、次式（１８）を用いて確認する（ステップＳ５０２）。

ｖｅｒｉｆｙ（ｐｃ，ｓｉｇｎ（ｓｃ，Ｒｅｆ２‖ＥＤＰＴ１‖Ｐｒ））　…（１８）

制御部４０１は、電子署名の正当性が確認できればステップＳ５０３へ進み、確認できない場合は、通信部３０５を介して商品部門ｃへ署名の正当性が確認できなかった旨を伝える（ステップＳ５０４）。

【００７１】次に、制御部３０１は、送られてきた（Ｒｅｆ２‖ＥＤＰＴ１‖Ｐｒ）［ｃ］に含まれている照会番号Ｒｅｆ２に基づいて、発注データ格納部３０６を検索し、当該照会番号Ｒｅｆ２と共に記録されている（ＲＥＤＰＴ２＝Ｆ（ｒｂ，ＥＰＤＴ１）
＝Ｆ（ｒｂ，Ｆ（ｒｃ，ＰＤＴ））　…（１９）

【００７３】次に、制御部３０１は、ＲＯＭ３０２から署名生成アルゴリズムｓｉｇｎを、秘密鍵保管部３０４から秘密鍵ｓｂを、それぞれ読み出し、照会番号Ｒｅｆ２と共に記録されている（Ｒｅｆ１‖ＥＯｒｄ１）

ｓｉｇｎ（ｓｂ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）　…（２０）

【００７４】次に、制御部３０１は、商品部門ｃから送られてきた（Ｒｅｆ２‖ＥＤＰＴ１‖Ｐｒ）［ｃ］を、（Ｒｅｆ１‖ＥＯｒｄ１）［ａ］と組にして発注データ格納部３０６に格納する（ステップＳ５０７）。次に、制御部３０１は、（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）［ｂ］を、受付部門ａに、通信部３０５からパソコン通信を用いて送信する（ステップＳ５０８）。

【００７５】受付部門ａは、パソコン通信を介して中継部門ｂから送られてきたデータ（Ｒｅｆ１‖ＥＰＤＴ２

ｖｅｒｉｆｙ（ｐｂ，ｓｉｇｎ（ｓｂ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ））
…（２１）

制御部２０１は、電子署名の正当性が確認できればステップＳ６０３へ進み、確認できない場合は、通信部２０６を介して中継部門ｂへ署名の正当性が確認できなかった旨を伝える（ステップＳ６０４）。

【００７６】次に、制御部２０１は、発注データ格納部２０７を検索して、中継部門ｂから送られてきた（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）［ｂ］からＲｅｆ１を取り出し、（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）［ｂ］を、ＩＤｉ

ｓｉｇｎ（ｓａ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）　…（２２）

【００７８】次に、制御部２０１は、照会番号Ｒｅｆ１とともに発注データ格納部２０７に格納されている個人識別子ＩＤｉを求め、そして当該ＩＤｉに対応するパソコン通信アドレスを個人データ格納部２０４から検索し、発注者ｉに、（Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）［ａ］を、通信部２０６からパソコン通信を用いて送信する（ステップＳ６０６）。

【００７９】発注者ｉは、パソコン通信を介して受付部門ａから送られてきたデータ（Ｒｅｆ１‖ＥＰＤＴ２‖

ｖｅｒｉｆｙ（ｐａ，ｓｉｇｎ（ｓａ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）；
…（２３）

る（ステップＳ５０２）。

ｖｅｒｉｆｙ（ｐｃ，ｓｉｇｎ（ｓｃ，Ｒｅｆ２‖ＥＤＰＴ１‖Ｐｒ））　…（１８）

ｅｆ１‖ＥＯｒｄ１）［ａ］から、図９のステップＳ３０３と同じようにして、乱数ｒｂを取り出す（ステップＳ５０３）。

【００７２】次に、制御部３０１は、ＲＯＭ３０２から秘密鍵暗号アルゴリズムＦを読み出し、鍵ｒｂを用いて、ＥＰＤＴ１を暗号化し、次式（１９）で示されるＥＰＤＴ２を生成する（ステップＳ５０５）。

ＥＰＤＴ２＝Ｆ（ｒｂ，ＥＰＤＴ１）
＝Ｆ（ｒｂ，Ｆ（ｒｃ，ＰＤＴ））　…（１９）

［ａ］から取り出した照会番号Ｒｅｆ１と、商品部門から送られてきたＥＰＤＴ２とＰｒとを連結した（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）に対し、次式（２０）を用いて、電子署名を施す（ステップＳ５０６）。

ｓｉｇｎ（ｓｂ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）　…（２０）

‖Ｐｒ）［ｂ］を、図３の通信部２０６を介して受信する（図１２のステップＳ６０１）。受付装置２０の制御部２０１は、ＲＯＭ２０２から、署名確認アルゴリズムｖｅｒｉｆｙと、中継部門ｂの公開鍵ｐｂとを読み出し、（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）［ｂ］の電子署名ｓｉｇｎ（ｓｂ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）が、（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）に対する中継部門ｂの電子署名であるか否かを、次式（２１）を用いて確認する（ステップＳ６０２）。

ｖｅｒｉｆｙ（ｐｂ，ｓｉｇｎ（ｓｂ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ））
…（２１）

およびＥＯｒｄ１［ｉ］と組にして、発注データ格納部２０７に記録する（ステップＳ６０３）。

【００７７】次に、制御部２０１は、ＲＯＭ２０２から署名生成アルゴリズムｓｉｇｎを、秘密鍵保管部２０５から秘密鍵ｓａを、それぞれ取り出し、Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒに対する電子署名を、次式（２２）を用いて生成する（ステップＳ６０５）。

ｓｉｇｎ（ｓａ，Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）　…（２２）

Ｐｒ）［ａ］を、図２の通信部１０９を介して受信する（図１３のステップＳ７０１）。物品購入装置１０の制御部１０１は、ＲＯＭ１０２から、署名確認アルゴリズムｖｅｒｉｆｙと、受付部門ａの公開鍵ｐａとを読み出し、（Ｒｅｆ１‖ＥＤＰＴ２‖ＺＰｒ）［ａ］の電子署名ｓｉｇｎ（ｓａ，Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）が、（Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）に対する受付部門ａの電子署名であるか否かを、次式（２３）を用いて確認する（ステップＳ７０２）。

ｖｅｒｉｆｙ（ｐａ，ｓｉｇｎ（ｓａ，Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）；
…（２３）

制御部１０１は、電子署名の正当性が確認できればステップＳ７０３へ進み、確認できない場合は、通信部１０９を介して受付部門ａへ署名の正当性が確認できなかった旨を伝える（ステップＳ７０４）。

【００８０】次に、制御部１０１は、送られてきた（Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）＾ａ＾からＲｅｆ１を取り出し、発注データ格納部１１０に格納されているＲｅｆ１［ａ］を検索し、その中で発注した商品の価格と、送られてきた（Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒ）＾ａ＾のＰｒとが一致するかどうか確かめる（ステップＳ７０５）。制御部１０１は、一致した場合は、ステップＳ７０５へ進み、一致しなかった場合は、通信部１０９を介して受付部門ａへ値段が違うとアピールする（ステップＳ７０６）。

【００８１】制御部１０１は、ＲＯＭ１０２から署名生成アルゴリズムｓｉｇｎを、秘密鍵保管部１０８から秘密鍵ｓｉを、それぞれ読み出し、Ｒｅｆ１‖ＥＤＰＴ２‖Ｐｒに対する電子署名を次式（２４）を用いて生成し、商品受取票Ｒｅｃｅｉｐｔとする（ステップＳ７０５）。

$$Receipt = sign(si, Ref1 \| EDPT2 \| Pr) \quad \cdots (24)$$

次に、制御部１０１は、商品受取票ＲｅｃｅｉｐｔをＲｅｆ１と共に、通信部１０９からパソコン通信を用いて、受付部門ａに送信する（ステップＳ７０７）。

【００８２】次に、制御部１０１は、ＲＯＭ１０２から秘密鍵復号アルゴリズムＦ＾ｄを読み出し、Ｒｅｆ１と組にして発注データ保管部に保管されている２つの乱数ｒｂ，ｒｃを読み出す。そして、制御部１０１は、次式（２５）のように、鍵ｒｂをＦ＾｛－１｝ｅに代入することにより、ＥＰＤＴ２を復号し、ＥＰＤＴ１を得る（ステップＳ７０８）。

$$F^{-1}(rb, EPDT2) = EPDT1 \quad \cdots (25)$$

次に、制御部１０１は、鍵ｒｃをＦ＾ｅに代入することにより、ＥＰＤＴ１を復号し、発注した電子的商品ＰＤＴを得る（ステップＳ７０９）。

$$F^{-1}(rc, EPDT1) = PDT \quad \cdots (26)$$

【００８３】なお、復号した商品ＰＤＴが発注したものと異なる場合は、制御部１０１は、パソコン通信を使って受付部門ａに商品違いをアピールする（ステップＳ７１０）。

【００８４】受付部門ａにおいて、制御部２０１は、発注者ｉ送られてきたＲｅｆ１が発注データ格納部２０７に記録されているかどうかを検索し、発注者ｉから送られてきたＲｅｃｅｉｐｔを、Ｒｅｆ１と共に格納されているＩＤｉ，ＥＯｒｄ１［ｉ］，（Ｒｅｆ１‖ＥＰＤＴ２‖Ｐｒ）と組にして保管する。そして、制御部２０１は、発注者ｉの予め登録されている振替指定銀行口座から、商品ＰＤＴの価格Ｐｒを引き落とし受付部門ａの口座に振替えるように、銀行に依頼する。

【００８５】次に、以上説明した通信ネットワークを用いた通信販売システムにおいて、＂誰が何を買ったのかわからない、というプライバシー保護が実現できていることについて述べる。まず初めに、受付部門ａ、中継部門ｂ、商品部門ｃの３つ全てが結託しないと「誰が何を買った」という情報がわからないことを示す。その後、各手続きにおいて、発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃが通常の手続きをしたかった場合の対策についても述べる。

【００８６】図１４は、先に説明した通信ネットワークを用いた通信販売システムにおいて、受付部門ａ、中継部門ｂ、商品部門ｃのそれぞれが、各手続きにおいて蓄積する情報のどれを知っているかを示している。○はその情報を保持していて、×は保持していないことを示している。

【００８７】発注者ｉの個人識別子ＩＤｉは、受付部門ａしか知らず、商品名ＰＩＤは商品部門ｃしか知らない。これは、商品に関する情報は、受付部門ａ、中継部門ｂでは暗号化された状態で処理されるからである。しかも、受付部門ａと商品部門ｃが共有している情報は、商品の価格Ｐｒしかないので、商品の価格がほとんど均一でしかも情報量が多いならば、仮に受付部門ａと商品部門ｃが互いに自分の持つ情報を相手に渡したとしても、それぞれが保持する情報を結び付ける情報がない。すなわち「誰が何を買ったのか」がわからない。また、中継部門ｂには、商品に関する情報も、発注者ｉに関する情報も無いので、受付部門ａ、商品部門ｃのいずれかと、互いに自分の持つ情報を相手に渡したとしても、「誰が何を買ったのか」がわからない。したがって、「誰が何を買った」という情報がわかるためには、受付部門ａ、中継部門ｂ、商品部門ｃの３つが結託し、互いに自分の持つ情報を相手に渡すことが必要となる。各部門が正常な組織倫理に基づいて運用される限り、３部門共が結託する可能性は非常に小さい。よって、＂誰が何を買ったのかわからない＂というプライバシー保護が実現できている。すなわち、発注者は匿名で通信ネットワークを介して商品を注文購入できる。

【００８８】次に、各手続きにおいて、発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃ（以下、単にまとめてセクションと呼ぶ）が通常の手続きをしなかった場合の対策について述べる。ここで、通常の手続きをしないとは、送られてきた情報を処理して次の手続へ送る際に、情報を改ざんしたりすることである。たとえば、先に説明した通信ネットワークを用いた通信販売システムにおいて、受付部門ａが発注者ｉから受け付けた暗号化発注内容ＥＯｒｄ１の内容の全部または一部を別のものにするといった場合がある。

【００８９】各手続きにおいて、各セクションが、送ら

35　　36

れてきた情報を書き替えて次の手続きへ送った場合は、各手続きにおいて情報を送る時に、そのセクションしか作成できない電子署名を一緒に送付している。電子署名は、送信途中で内容が改ざんされた場合でも署名確認時に判明する。すなわち、各セクションの発注データ格納部には、送られてきた情報とその電子署名が格納されているため、その情報を元にたどっていけば誰が情報を書き換えたかが判明する。したがって、各セクションは、情報を無断で書き換えることができない。

【００９０】以上説明したように、上記実施例の通信ネットワークを用いた通信販売システムにおいては、「誰が何を買ったのかわからない」というプライバシー保護が実現できていて、発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃのいずれかが通常の手続きをしなかった場合も、そのような手続きをどの部門で行ったかが特定できる。

【００９１】なお、上記実施例においては、発注者ｉ、受付部門ａ、中継部門ｂ、商品部門ｃの双方向通信を、パソコン通信を用いて行なっているが、デジタルＣＡＴＶ網、Ｂ－ＩＳＤＮなどの双方向通信が行なえる他の通信ネットワークを採用してもよく、この場合も上記実施例と同様の効果が得られる。

【００９２】また、上記実施例においては、発注者ｉから受付部門ａへの商品代金の受渡しを、システム申込時に振替指定銀行口座をシステム管理者に知らせ、受付部門ａがその振替指定銀行口座から受付部門ａの口座へ振り替えてもらうように銀行に依頼することで実現しているが、システム加入時に予め発注者ｉが加入しているクレジットカード部門の会員番号を知らせ、受付部門ａは商品代金を指定されたクレジット部門から立て替え払いしてもらうことで実現してもよく、この場合も上記実施例と同様の効果が得られる。

【００９３】また、上記実施例においては、受付部門ａと商品部門ｃとの間に中継部門ｂを設定しているが、中継部門を省略することもできる。この場合、受付部門ａは発注者が誰であるかを特定できるが、発注内容ならびに商品そのものは暗号化されているので何を買ったのかを特定できない。また、商品部門ｃは、何を買ったのかは特定できるが、受付部門ａから送られてくる照会番号は発注者とは対応づけられない。すなわち、誰が買ったのかを特定できない。よって、この場合も、いずれの部門も、単独では「誰が何を買ったのか」がわからず、プライバシー保護が実現できている。

【００９４】また、上記実施例においては、購入する商品を電子的商品としたが、電子的ではない一般的な商品に対しても、プライバシーを保護する本発明の通信ネットワークを用いた通信販売システムを適用することが可能である。ただし、この場合、上記実施例の手続きを若干手変更する必要がある。このことを以下に述べる。

【００９５】発注者ｉが商品を発注して、その発注情報を受付部門ａが受け付けて、中継部門ｂを介して、商品部門ｃにパソコン通信を用いて送るところまでは同じである。しかしながら、電子的ではない一般的な商品は暗号化できないので、商品部門ｃは、商品を物理的に包装した後、商品部門ｃしか持っていない用紙で封印をして、当該封印された商品をＲｅｆ２と共に、中継部門ｂに物理的に送る。中継部門ｂでは、送られてきた商品部門ｃの封印のついた商品を、さらに包装し、中継部門ｂしか持っていない用紙で封印する。そして、当該二重に封印された商品を、Ｒｅｆ２に対応するＲｅｆ１と共に受付部門ａに物理的に送る。受付部門ａは、二重に封印された商品を、発注者ｉに物理的に届ける。また、上記実施例においては、商品部門ｃから中継部門ｂおよび受付部門ａを介して、発注者ｊに商品を送付する際に、電子署名を付加して送信しているが、この点は、物品受領書と通常の印鑑に変わる。

【００９６】上記のように、電子的ではない一般的な商品に対しても、プライバシーを保護する本発明の通信ネットワークを用いた通信販売システムを適用することが可能である。

【００９７】また、上記実施例においては、中継部門を１つとして説明したが、中継部門を複数設けたシステム、すなわち第１～第ｎ（ｎは２以上の整数）の中継部門を設けるシステムにも本発明を適用することが可能である。ただし、この場合、上記実施例の手続きを若干変更する必要があるので、以下にこのことを述べる。

【００９８】上記実施例における中継部門ｂは、第１の中継部門ｂ１が代わる。この時、第１の中継部門ｂ１から直接に商品部門ｃに、

（Ｒｅｆ２‖ＥＯｒｄ２）［ｂ１］

を送るのではなく、第２の中継部門ｂ２から第ｎの中継部門ｂｎを介して送られる。すなわち、第ｍの中継部門ｂｍから第（ｍ＋１）の中継部門ｂ（ｍ＋１）へは、

（Ｒｅｆ（ｍ－１）‖ＥＯｒｄ２）［ｂｍ］

が送信される。ただし、Ｒｅｆ（ｍ－１）は、第（ｍ＋１）の照会番号である。また、Ｒｅｆ１からＲｅｆ（ｎ＋１）までは、各値がすべて異なる。そして、第ｎの中継部門ｂｎから商品部門ｃへは、

（Ｒｅｆ（ｎ－１）‖ＥＯｒｄ２）［ｂｎ］

が送られる。商品部門ｃでは、受信した（Ｒｅｆ（ｎ＋１）‖ＥＯｒｄ２）［ｂｎ］からＰＩＤを得て、ＰＤＴを暗号化し、

（Ｒｅｆ（ｎ－１）‖ＥＰＤＴ１‖Ｐｒ）［ｃ］

を第ｎの中継部門ｂｎへ送信する。また、第ｍの中継部門ｂｍから第（ｍ－１）の中継部門ｂ（ｍ－１）へは、

（Ｒｅｆ（ｍ－１）‖ＥＰＤＴ１‖Ｐｒ）［ｂｍ］

が送信される。そして、第１の中継部門ｂ１から受付部門ａには、

（Ｒｅｆ２‖ＥＰＤＴ１‖Ｐｒ）［ｂ１］

が送信される。以下の手順は、上記実施例と同じであ

る。この場合のプライバシーの安全性は、上記実施例の安全性のところで述べたように、各部門の結託の可能性に依存しており、その可能性は上記実施例に比べて低くなる。

【００９９】また、上記実施例では、受付部門ａ、中継部門ｂ、商品部門ｃを、１つの会社内に設けるようにしたが、これら各部門を別会社として組織するようにしてもよい。

【０１００】

【発明の効果】請求項１の発明によれば、受付部門は、発注者の発注した商品の内容および商品部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。したがって、受付部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落しなどの既存の決裁システムをそのまま使用することができる。

【０１０１】請求項２の発明によれば、仮名情報として、各注文毎に異なる情報を使用しているので、商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【０１０２】請求項３の発明によれば、受付部門は、発注者の発注した商品の内容および中継部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。また、中継部門は、発注者の発注した商品の内容および商品部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。さらに、中継部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる第１の仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。したがって、受付部門と中継部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。なお、受付部門と商品部門が結託しようとしても、両部門の持っている情報を結び付ける情報がないので、結託しようがない。したがって、結託によるプライバシーの侵害を有効に防止することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落しなどの既存の決裁システムをそのまま使用することができる。

【０１０３】請求項４の発明によれば、第１および第２の仮名情報として、各注文毎に異なる情報を使用しているので、中継部門または商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【０１０４】請求項５の発明によれば、中継部門が複数設けられ、商品の発注内容および発注された商品がこれら複数の中継部門を介して伝達されるので、各部門の結託がより一層困難になり、発注者のプライバシーをより確実に保護することができる。

【０１０５】請求項６の発明によれば、受付部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また商品部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。したがって、受付部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落しなどの既存の決裁システムをそのまま使用することができる。

【０１０６】請求項７の発明によれば、仮名情報として、各注文毎に異なる情報を使用しているので、商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【０１０７】請求項８の発明によれば、受付部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また中継部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。また、中継部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また商品部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。さらに、中継部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる第１の仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、第１の仮名情報とは異なる第２の仮名情報が付加されて送られてくるので、誰が商品を発注したかを知ることができない。したがって、受付部門と中継部門と商品部門とが結託しない

限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。なお、受付部門と商品部門が結託しようとしても、両部門の持っている情報を結び付ける情報がないので、結託しようがない。したがって、結託によるプライバシーの侵害を有効に防止することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落しなどの既存の決裁システムをそのまま使用することができる。

【０１０８】請求項９の発明によれば、中継部門が複数設けられ、商品の発注内容および発注された商品がこれら複数の中継部門を介して伝達されるので、各部門の結託がより一層困難になり、発注者のプライバシーをより確実に保護することができる。

【図面の簡単な説明】

【図１】本発明の一実施例に係る通信ネットワークを用いた通信販売システムの構成を示すブロック図である。

【図２】図１に示す発注者ｉに設けられた物品購入装置１０の構成の一例を示すブロック図である。

【図３】図１に示す受付部門ａに設けられた受付装置２０の構成の一例を示すブロック図である。

【図４】図１に示す中継部門ｂに設けられた中継装置３０の構成の一例を示すブロック図である。

【図５】図１に示す商品部門ｃに設けられた商品発送装置４０の構成の一例を示すブロック図である。

【図６】図１に示す通信ネットワークを用いた通信販売システム全体の動作を示すシーケンスチャートである。

【図７】図１の物品購入装置１０の商品発注時の動作を示すフローチャートである。

【図８】図１の受付装置２０の発注受付時の動作を示すフローチャートである。

【図９】図１の中継装置３０の発注中継時の動作を示すフローチャートである。

【図１０】図１の商品発送装置４０の動作を示すフローチャートである。

【図１１】図１の中継装置３０の商品中継時の動作を示すフローチャートである。

【図１２】図１の受付装置２０の商品発送時の動作を示すフローチャートである。

【図１３】図１の物品購入装置１０の商品受け取り時の動作を示すフローチャートである。

【図１４】図１の実施例において、各部門で知り得る情報を説明するための図である。

【図１５】従来の通信ネットワークを用いた通信販売システムの構成の一例を示すブロック図である。

【符号の説明】

１…発注者

１０…物品購入装置

２…受付部門

２０…受付装置

３…中継部門

３０…中継装置

４…商品部門

４０…商品発送装置

１０１，２０１，３０１，４０１…制御部

１０２，２０２，３０２，４０２…ＲＯＭ

１０３，２０３，３０３，４０３…ＲＡＭ

１０４…入力操作器

１０５…表示器

１０６…商品カタログ格納部

１０７…乱数発生部

１０８，２０５，３０４，４０４…秘密鍵保管部

１０９，２０６，３０５，４０５…通信部

１１０，２０７，３０６，４０６…発注データ格納部

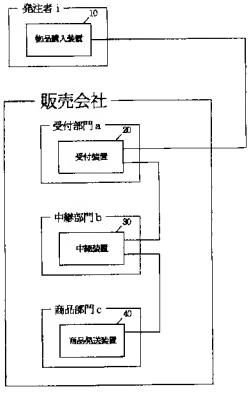
２０４…個人データ格納部

２０８，３０７…照会番号発行部

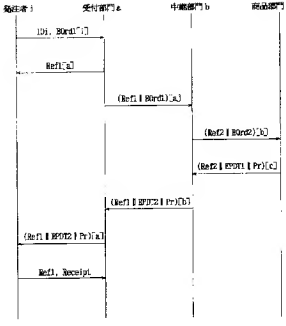
４０７…商品データ格納部

４０８…商品保管部

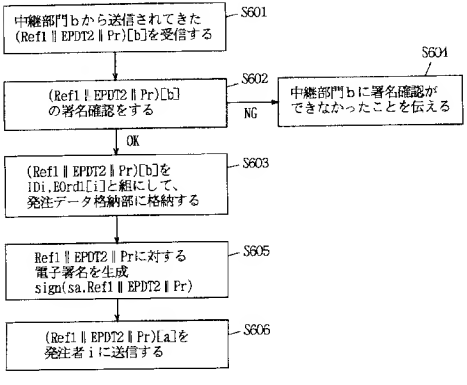
【図１】


発注者ｉ
10
他企業購入装置
販売会社
受付部門ａ
20
受付装置
中継部門ｂ
30
中継装置
商品部門ｃ
40
商品発送装置

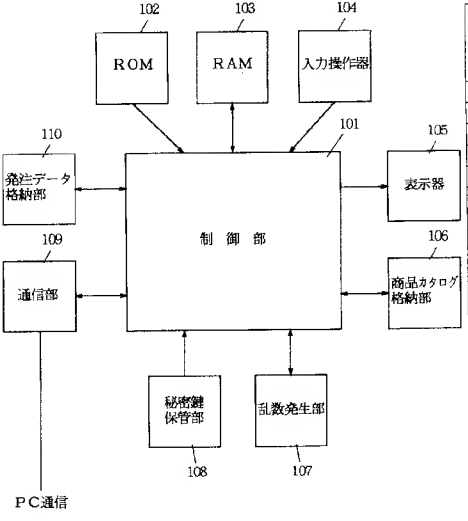
【図６】


発注者ｉ
受付部門ａ
中継部門ｂ
商品部門ｃ
IDi, EOrdl[i]
Ref1[a]
(Ref1 ‖ EOrdl)[a]
(Ref2 ‖ EOrd2)[b]
(Ref2 ‖ EPDT1 ‖ Pr)[c]
(Ref1 ‖ EPDT2 ‖ Pr)[b]
(Ref1 ‖ EPDT2 ‖ Pr)[a]
Ref1, Receipt

【図１２】


中継部門ｂから送信されてきた
(Ref1 ‖ EPDT2 ‖ Pr)[b]を受信する
S601
(Ref1 ‖ EPDT2 ‖ Pr)[b]
の署名確認をする
S602
NG
S604
中継部門ｂに署名確認が
できなかったことを伝える
OK
(Ref1 ‖ EPDT2 ‖ Pr)[b]を
IDi,EOrdl[i]と組にして、
発注データ格納部に格納する
S603
Ref1 ‖ EPDT2 ‖ Prに対する
電子署名を生成
sign(sa,Ref1 ‖ EPDT2 ‖ Pr)
S605
(Ref1 ‖ EPDT2 ‖ Pr)[a]を
発注者ｉに送信する
S606

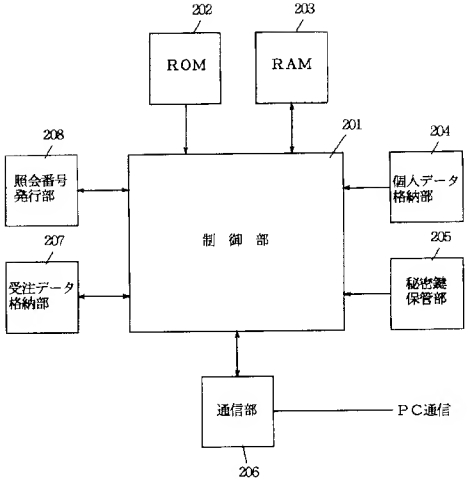
【図２】



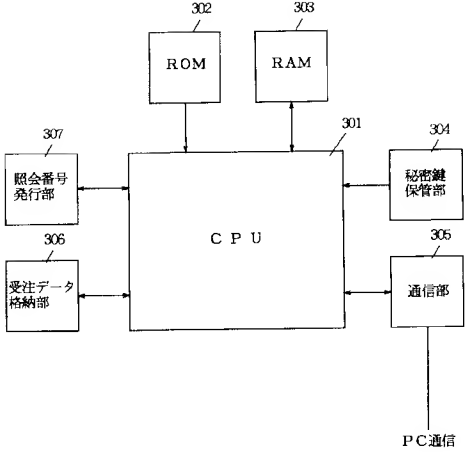
【図１４】

	受付部門 a	中継部門 b	商品部門 c
IDi	○	×	×
PID	×	×	○
Pr	○	○	○
Ref1	○	○	×
Ref2	×	○	○
rb	×	○	×
rc	×	×	○
RDrd1	○	○	×
RDrd2	×	○	○
RPD1	×	○	○
RPD2	○	○	×

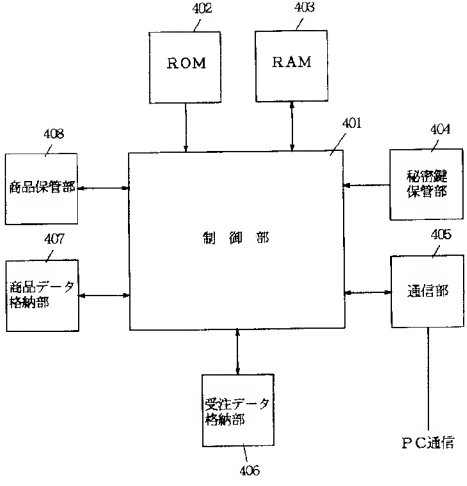
【図３】


202
203
ROM
RAM
201
208
照会番号
発行部
204
個人データ
格納部
制　御　部
207
受注データ
格納部
205
秘密鍵
保管部
通信部
ＰＣ通信
206

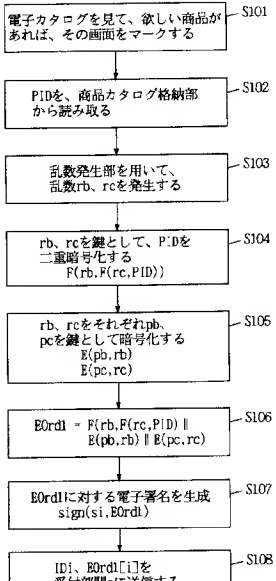
【図４】


302
303
ROM
RAM
301
307
照会番号
発行部
304
秘密鍵
保管部
C P U
306
受注データ
格納部
305
通信部
PC通信

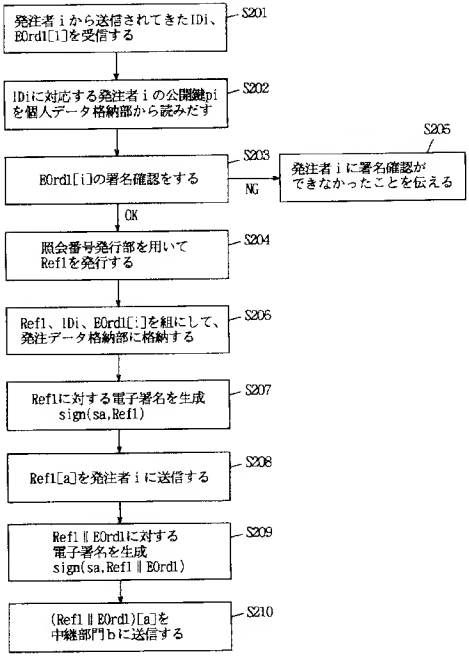
【図５】


402
403
ROM
RAM
401
408
404
商品保管部
秘密鍵
保管部
制　御　部
407
405
商品データ
格納部
通信部
受注データ
格納部
406
ＰＣ通信

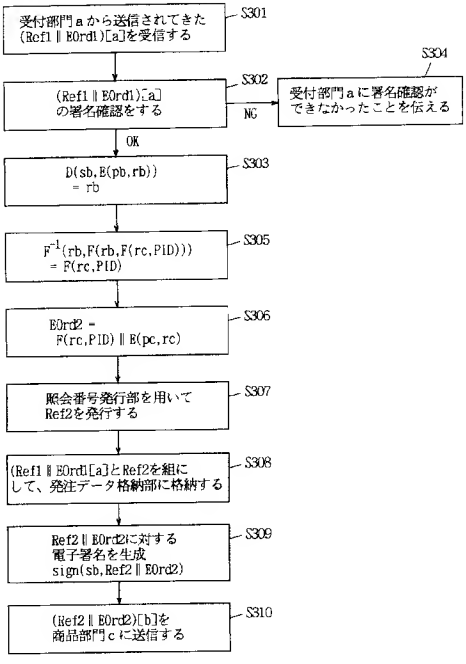
【図7】


電子カタログを見て、欲しい商品があれば、その画面をマークする
S101
PIDを、商品カタログ格納部から読み取る
S102
乱数発生部を用いて、乱数rb、rcを発生する
S103
rb、rcを鍵として、PIDを二重暗号化する
F(rb,F(rc,PID))
S104
rb、rcをそれぞれpb、pcを鍵として暗号化する
E(pb,rb)
E(pc,rc)
S105
EOrdl = F(rb,F(rc,PID)) ‖ E(pb,rb) ‖ E(pc,rc)
S106
EOrdlに対する電子署名を生成
sign(si,EOrdl)
S107
IDi、EOrdl[i]を受付部門aに送信する
S108

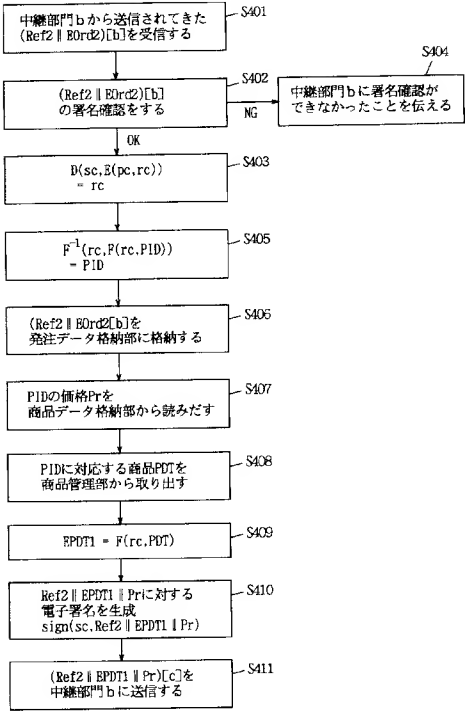
【図8】


発注者ｉから送信されてきたIDi、EOrdl[i]を受信する
S201
IDiに対応する発注者ｉの公開鍵piを個人データ格納部から読みだす
S202
EOrdl[i]の署名確認をする
S203
NG
発注者ｉに署名確認ができなかったことを伝える
S205
OK
照会番号発行部を用いてRe f lを発行する
S204
Re f l、IDi、EOrdl[:]を組にして、発注データ格納部に格納する
S206
Re f lに対する電子署名を生成sign(sa,Re f l)
S207
Re f l[a]を発注者ｉに送信する
S208
Re f l‖EOrdlに対する電子署名を生成sign(sa,Re f l‖EOrdl)
S209
(Re f l‖EOrdl)[a]を中継部門bに送信する
S210

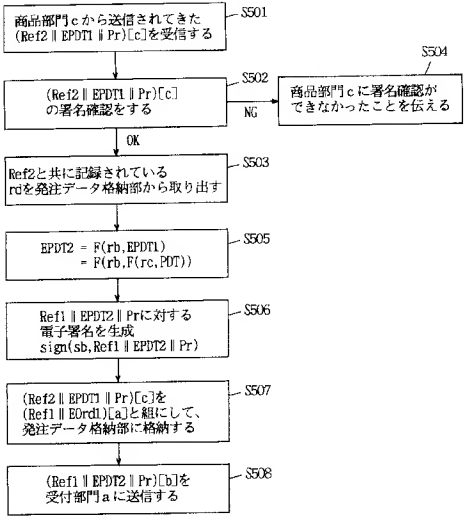
【図９】


受付部門ａから送信されてきた
(Ref1 ‖ EOrd1)[a]を受信する
S301
(Ref1 ‖ EOrd1)[a]
の署名確認をする
S302
NG
S304
受付部門ａに署名確認が
できなかったことを伝える
OK
D(sb,E(pb,rb))
= rb
S303
F^-1(rb,F(rb,F(rc,PID)))
= F(rc,PID)
S305
EOrd2 =
F(rc,PID) ‖ E(pc,rc)
S306
照会番号発行部を用いて
Ref2を発行する
S307
(Ref1 ‖ EOrd1[a]とRef2を組に
して、発注データ格納部に格納する
S308
Ref2 ‖ EOrd2に対する
電子署名を生成
sign(sb,Ref2 ‖ EOrd2)
S309
(Ref2 ‖ EOrd2)[b]を
商品部門ｃに送信する
S310

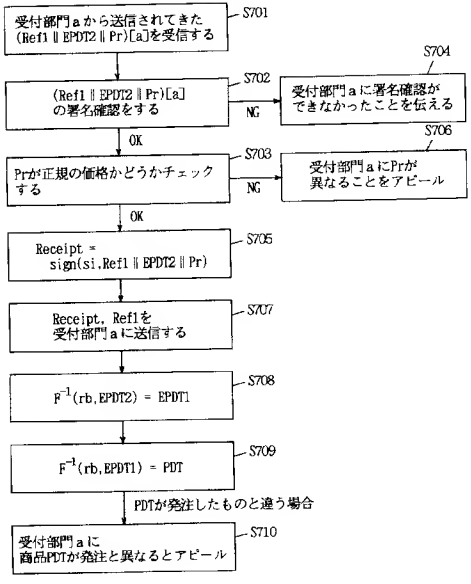
【図１０】


中継部門ｂから送信されてきた
(Ref2 ‖ EOrd2)[b]を受信する
S401
(Ref2 ‖ EOrd2)[b]
の署名確認をする
S402
NG
S404
中継部門ｂに署名確認が
できなかったことを伝える
OK
D(sc,E(pc,rc))
= rc
S403
F-1(rc,P(rc,PID))
= PID
S405
(Ref2 ‖ EOrd2[b]を
発注データ格納部に格納する
S406
PIDの価格Prを
商品データ格納部から読みだす
S407
PIDに対応する商品PDTを
商品管理部から取り出す
S408
EPDT1 = F(rc,PDT)
S409
Ref2 ‖ EPDT1 ‖ Prに対する
電子署名を生成
sign(sc,Ref2 ‖ EPDT1 ‖ Pr)
S410
(Ref2 ‖ EPDT1 ‖ Pr)[c]を
中継部門ｂに送信する
S411

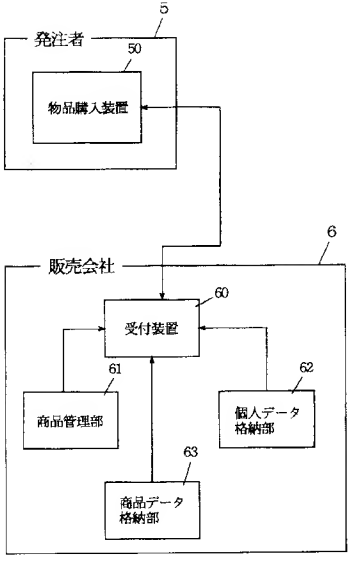
【図１１】


商品部門ｃから送信されてきた
(Ref2 ‖ EPDT1 ‖ Pr)[c]を受信する
S501
(Ref2 ‖ EPDT1 ‖ Pr)[c]
の署名確認をする
S502
NG
S504
商品部門ｃに署名確認が
できなかったことを伝える
OK
Ref2と共に記録されている
rdを発注データ格納部から取り出す
S503
EPDT2 = F(rb,EPDT1)
= F(rb,F(rc,PDT))
S505
Ref1 ‖ EPDT2 ‖ Prに対する
電子署名を生成
sign(sb,Ref1 ‖ EPDT2 ‖ Pr)
S506
(Ref2 ‖ EPDT1 ‖ Pr)[c]を
(Ref1 ‖ EOrd1)[a]と組にして、
発注データ格納部に格納する
S507
(Ref1 ‖ EPDT2 ‖ Pr)[b]を
受付部門ａに送信する
S508

【図13】


受付部門aから送信されてきた
(Ref1 ‖ EPDT2 ‖ Pr)[a]を受信する
S701
(Ref1 ‖ EPDT2 ‖ Pr)[a]
の署名確認をする
S702
NG
受付部門aに署名確認が
できなかったことを伝える
S704
OK
Prが正規の価格かどうかチェック
する
S703
NG
受付部門aにPrが
異なることをアピール
S706
OK
Receipt =
sign(si,Ref1 ‖ EPDT2 ‖ Pr)
S705
Receipt, Ref1を
受付部門aに送信する
S707
F-1(rb,EPDT2) = EPDT1
S708
F-1(rb,EPDT1) = PDT
S709
PDTが発注したものと違う場合
受付部門aに
商品PDTが発注と異なるとアピール
S710

【図１５】



フロントページの続き

(51)Int.Cl.'	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　17/60				
Ｇ０９Ｃ　1/00		7259－５Ｊ		